REPORT

Russia's Electronic Warfare Capabilities to 2025

Challenging NATO in the Electromagnetic Spectrum

Roger N. McDermott | with a foreword by General Michael Hayden

September 2017

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Republic of Estonia
Ministry of Defence

Title: Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum
Author: McDermott, Roger N.
Project director: Jermalavičius, Tomas
Publication date: September 2017
Category: Report
Keywords: Anti-Access/Area Denial (A2/AD), Capabilities & Capability Planning, Command & Control, Electronic Warfare, Defence Acquisition, Defence Industry, NATO, Russia, Ukraine, Syria, Georgia

Photos:
Cover page—Russian soldiers erect an antenna of a *Krasukha*-4 EW complex.
Page VII—Control panel of a *Krasukha*-4 EW complex.
Page 31—Inside an antenna section of a *Krasukha*-4 EW complex.
Source: *Voyennoye Obozreniye* ("Military Review"), https://topwar.ru/93268-armiya-2016-reb-kompleks-krasuha-4.html

Disclaimer: This report was supported by a research grant provided by the Estonian Ministry of Defence. The views and opinions contained in this report are those of its author only and do not necessarily represent the official policy or position of the International Centre for Defence and Security or Estonian Ministry of Defence.

ISSN 2228-0529
ISBN 978-9949-9885-9-4 (print)
978-9949-9972-0-6 (PDF)

63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Foreword

When the Russian army stormed into Georgia in August 2008, we lacked detailed knowledge of its capabilities. Our technical systems were even challenged to locate the limits of the Russian advance. In 2014 the Russians, their "little green men" and their concept of hybrid war surprised us again with the rapid seizure of Crimea and the occupation of part of the Donbas region in Ukraine. This same Russian army is today in a position to threaten the Baltic states and NATO's entire eastern flank. The time for surprises should be over.

Thankfully, the International Centre for Defence and Security in Estonia has created a detailed, fact-based study on one critical aspect of Russia's growing capabilities: Electronic Warfare (EW). Moscow relies on—and has heavily invested in—EW as an asymmetrical response to NATO's technological edge across the spectrum of conflict and as an integral part of its anti-access/area denial strategy. If Moscow can negate NATO's command, control and intelligence systems, it will make the Alliance's defence of its new members problematic and costly.

Thus, ICDS's study could not be more timely. This is a professional work that catalogues the seriousness of the threat without being unduly alarmist. It is fact based, from the detailed descriptions of Russian equipment and investment; through Moscow's development of organisation and command structure; to accounts of training, tactics and operations. There is also a great discussion of Russian doctrine and how Russian EW fits into broader questions of cyber and psychological operations and how that convergence will further challenge NATO's concepts and practices.

I highly recommend this important work as the departure point for the Alliance rethinking and reshaping its response to a growing danger.

General (retired) **Michael HAYDEN**

Former Director of the US National Security Agency (NSA)
and Central Intelligence Agency (CIA)

Acknowledgments

The author wishes to express his grateful appreciation to the staff and leadership of the ICDS and Estonian Ministry of Defence for making this study possible, and to the interviewed experts for sharing their knowledge and offering candid and insightful comments.

About the Author

Roger N.McDermott joined the International Centre for Defence and Security in April 2016 as a Non-Resident Research Fellow. He is a Senior Fellow in Eurasian Military Studies, The Jamestown Foundation, Washington DC, Senior International Research Fellow for the Foreign Military Studies Office (FMSO), Fort Leavenworth, Kansas, USA, and Research Associate, the Institute of Middle East, Central Asia and Caucasus Studies (MECACS), University of St. Andrews, Scotland, UK. Roger N. McDermott is on the editorial boards of *Russian Law & Politics, Central Asia and the Caucasus* and the scientific board of the *Journal of Power Institutions in Post-Soviet Societies*. His weekly assessments of military, security and strategic developments in Russia and Central Asia appear in *Eurasia Daily Monitor*, the flagship publication of The Jamestown Foundation.

Roger N. McDermott specialises in Russian and Central Asian defence and security issues. His interests in Russia's defence and security developments are mainly in the areas of defence reform, force structure, training, strategic exercises, military theory, perspectives on future warfare, planning and combat capability and readiness, as well as operational analysis. Among his numerous publications are the following: *Brothers Disunited: Russia's Use of Military Power in Ukraine*, (Eds., J.L. Black and Michael Johns), *Return of the Cold War. Ukraine, the West, and Russia*, Routledge: London, 2016; (Editor) *The Transformation of Russia's Armed Forces: Twenty Lost Years*, London: Routledge, 2014, and co-editor with Bertil Nygren and Carolina Vendil-Pallin, *The Russian Armed Forces in Transition: Economic, Geopolitical and Institutional Uncertainties*, Routledge: London, 2011. His latest report, co-authored with Tor Bukkvoll, is *Russia in the Precision-Strike Regime: Military Theory, Procurement, and Operational Impact*, FFI, 2017.

Executive Summary

- Russia's Armed Forces' electronic warfare (EW) capability development will pose a serious challenge to the proper planning and execution of NATO's defence of the Baltic states, and NATO's entire Eastern Flank, in the event of a Russian assault. This capability is an integral part of Russia's anti-access/area denial (A2/AD) approach and is clearly tailored to target NATO's C4ISR.

- Russia's growing technological advances in EW will allow its forces to jam, disrupt and interfere with NATO communications, radar and other sensor systems, Unmanned Aerial Vehicles (UAVs) and other assets, thus negating advantages conferred on the Alliance by its technological edge. Be it in the air, maritime, land or cyber domains, NATO will encounter an increasingly capable adversary focused on developing and deploying a vast array of EW systems as "force enablers and multipliers". Many of those systems are being introduced in units across all services stationed in Western Military District (MD) adjacent to NATO's borders.

- Moscow's interest in boosting EW capabilities vis-à-vis NATO has its origins in seeking to asymmetrically challenge the Alliance on Russia's periphery and maximise its chances of success in any operation against NATO's eastern members. Russia has consistently invested in EW modernisation since 2009, with modernised EW systems entering service across strategic, operational and tactical levels to augment capabilities of all service branches and arms. Modernisation of the EW inventory is set to continue in the State Armaments Programme up to 2025, which means Russia's military will benefit greatly from further advances in EW capability.

- Moscow is stepping up its efforts to renew and modernise the EW inventory, and this effort is complemented by changes to organisation, doctrine, command structure, training and tactics, as well as techniques and procedures. The effect of those changes is evident in Russia's aggression against Ukraine, where EW forms an organic part of Russia's kinetic and non-kinetic operations—both in support of proxy forces and conducted independently.

- Russia is actively developing a "total package" of EW systems to include a broad frequency range and other systems; these seem advanced and capable. In addition to such systems covering surveillance, protection and countermeasures (jamming), they cover measures to protect Russia's own usage of the electromagnetic spectrum (EMS). These systems also offer countermeasures against "Western" civilian and military usage of the EMS. Many of these Russian EW systems are highly mobile, including small systems deployable by UAVs, making targeting and neutralising them more complex and challenging.

- NATO must understand that Russia's interest in and use of EW is part of a wider effort by Moscow to adopt and strengthen its network-centric capability, which focuses upon C4ISR integration. Russia is already fielding automated command and control (C2) systems that are feeding into EW capability. For example, the *Baikal*-1ME brigade/regiment-level automated system is interoperable with systems used by EW units. Moreover, these are highly mobile, rendering them difficult to locate. Such developments allow, for instance, Russian forces to

establish a highly integrated air defence network and thus improve response times, promote situational awareness and enhance coordination between force elements.

- NATO's planners must also understand that the Russian EW capability extends well beyond air defence or even A2/AD, as it is fielding a wider array of systems to assist, for example, psychological operations (PSYOPS) and cyber operations. This capability deployed against Ukrainian government forces and enabling access to soldiers' means of communications aims to undermine and degrade troops' morale. Russia's ability to contest the EMS, combined with its holistic military thinking, means that EW capability will be exploited and effects created well beyond the traditional realms in which NATO's thinking about EW is rooted. We might witness an ever-growing convergence of Russia's EW, cyber- and information warfare approaches, which will further challenge NATO's concepts and practices.

- As a result, NATO needs to plan, revise its scenarios, and train to conduct defensive and offensive operations in a fiercely contested EMS battlespace. In their current form, NATO plans to defend its Eastern Flank including the Baltic states are inadequate as they do not take account of the full spectrum of Russia's current and future EW capabilities and their uses—as part of A2/AD approach and beyond. The Alliance must strengthen those plans to take account of advances in and possible future evolution of Russian EW capability, and this is more vital and pressing than efforts to boost the Alliance's cyber- and information warfare capability. NATO's Enhanced Forward Presence and further development of its posture in the Baltic area, which might possibly include assets for integrated air and missile defence, will fail to deliver the desired outcome if the Alliance falls behind in the contest for EMS dominance.

- The Alliance could also help the armed forces of the Baltic states—which are "tech-savvy" and eager to learn and develop their national capabilities—over how to counter EW measures and operate successfully in a highly contested EMS battlespace. There should be more support for enhancing their technical competence, developing concepts and doctrines, facilitating technology transfers, acquiring capabilities and training the forces. The Baltic states could work more closely with Israel, as its defence forces and industry have greatly benefited from their relationship with the United States and developed the posture, competence and capability required to cope with the EW challenge.

List of Abbreviations

A2/AD	Anti-Access/Area Denial
AEW&C	Airborne Early Warning and Control
ATO	Anti-Terrorist Operation
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
COMINT	Communications Intelligence
DRFM	Digital Radio Frequency Memory
EA	Electronic Attack
ECM	Electronic Counter Measures
EIB	Electronic Information Blocking
ELINT	Electronic Intelligence
EMP	Electro-Magnetic Pulse
EP	Electronic Protection
EMS	Electromagnetic Spectrum
ES	Electronic Support
EW	Electronic Warfare
GSM	Global System for Mobile (communications)
GPS	Global Positioning System
GPV	*Gosudarstvennaya Programma Vooruzheniya* (State Armaments Programme)
HF	High Frequency
HQ	Headquarters
IED	Improvised Explosive Device
IFF	Identification Friend of Foe
ISR	Intelligence, Surveillance and Reconnaissance
ITOK	*Integrirovannyy Trenazherno-Obuchayushchiy Kompleks* (Integrated Training and Learning System)
IW	Information Warfare
KRET	*Kontsern Radioelektronnye Tekhnologii* (Radio-Electronic Technologies Concern)
KTK	*Kompleksny Tekhnicheskiy Kontrol'* (Integrated Technical Control)
MD	Military District
MRB	Motorised Rifle Brigade
NATO	North Atlantic Treaty Organisation
NHW	Nuclear Homing Weapon
NTT	*Nauchno-Tekhnicheskiy Tsentr* (Scientific-Technical Centre)
OSCE	Organisation for Security and Cooperation in Europe
OSK	*Obyedinyonnoye Strategicheskoye Komandovaniye* (Joint Strategic Command)
REB	*Radioelektronnaya Bor'ba* (Radio-Electronic Combat)
PSYOPS	Psychological Operations
R&D	Research and Development
RVSN	*Raketnyye Voyska Strategicheskogo Naznacheniya* (Strategic Rocket Forces)
SEAD	Suppression of Enemy Air Defences
SIGINT	Signals Intelligence
SAA	Syrian Arab Army
SINGGARS	Single Channel Ground and Airborne Radio System
SMM	Special Monitoring Mission
STT	*Spetsialnyy Tekhnologicheskiy Tsentr* (Special Technology Centre)
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aerial System
UHF	Ultra High Frequency
VDV	*Vozdushno-Desantnye Voyska* (Airborne Forces)
VHF	Very High Frequency
VKS	*Vozdushno-Kosmicheskiye Sily* (Aerospace Forces)
VTA	*Voyenno-Transportnaya Aviatsiya* (Military Transport Aviation)
WFF	War Fighting Functions

ПОРЯДОК ВКЛЮЧЕНИЯ ИЗДЕЛИЯ

– на ЩС1 МПП выключатель автоматический "КР2 – ОТКЛ" перевести в положение "КР2";
– на ЩС2 МПП выключатель автоматический "ЭМУ – ОТКЛ" перевести в положение "ЭМУ";
– на ЩС3 МПП выключатели автоматические "ВЕНТ Ст – ОТКЛ", "АППАРАТУРА 220В 400Гц – ОТКЛ" перевести в положение "ВЕНТ Ст", "АППАРАТУРА 220В 400Гц" соответственно;
– на БПЗЭ ПУ и БПЭЭ МПП выключатели автоматические "СЕТЬ – ОТКЛ", "ТРАНСФОРМАТОР – ОТКЛ" перевести в положение "СЕТЬ", "ТРАНСФОРМАТОР" соответственно и проконтролировать загорание индикаторных ламп "Трансформатор" и "24В";
– на блоке пульта управления АСГ установить тумблер "УПР АРМ – ПУ" в положение "ПУ", тумблер "РУЧН – АВТ" в положение "АВТ", тумблер "ПУ – ОТКЛ" в положение "ПУ";
– включить навигационную аппаратуру "14Ц853", нажав кнопку " ⏻ " на приемнике навигационном индивидуальном;
– на ЩПР ПУ выключатели автоматические "РС1 – ОТКЛ", "РС2 – ОТКЛ", "ОСВЕЩЕНИЕ РМ – ОТКЛ", "АПД – ОТКЛ", "РЕГИСТРАЦИЯ УД – ОТКЛ" перевести в положения "РС1", "РС2", произвести включение АРМ1 и АРМ2, для чего:
– на ЩПР ПУ выключатели автоматические "АРМ1 – ОТКЛ", "АРМ2 – ОТКЛ" перевести в положения "АРМ1", "АРМ2" соответственно;
– на панели управления ЭВМ (ПУ ЭВМ) АРМ1, АРМ2 тумблер "ПИТАНИЕ – ОТКЛ" перевести в положение "ПИТАНИЕ";
– на панели управления МПП (ПУ МПП) АРМ1 (АРМ2) нажать кнопку "ВКЛ";
– на радиостанции Р–168–100У–2 тумблер "ПИТАНИЕ – ВКЛ" перевести в положение "ВКЛ";
– снять рамку ограждения ОПУ в МПП, закрыть люк по левому борту кузова МПП;
– на панели управления МПП (ПУ МПП) АРМ1 (АРМ2) нажать кнопки "ПРИВОД АЗИМУТ ВКЛ", "УГОЛ МЕСТА ВКЛ";
– после подачи питания на АРМ1 и АРМ2 выполняется процедура запуска ЭВМ.

АВТОКОНТРОЛЬ ИЗДЕЛИЯ

– загрузить на главной экранной форме (ЭФ) режим работы "Контроль F4";
– выполнить комплексную проверку оборудования ПУ, для чего нажать на кнопку "ПУ (F4)" "Контроль", а затем на кнопку "Автоконтроль (Ctrl+A)".

3. Выполнить комплексную проверку оборудования МПП, для чего:
а) нажать на кнопку "МПП (F2)" на ЭФ "Контроль", а затем на кнопку "Автоконтроль (Ctrl+A)";
б) нажать на кнопку "Запуск" в панели "Контроль ПРЧ";
Результаты тестирования выводятся в окне сообщений и отображаются на соответствующих индикаторах состояния зеленым (исправно) или красным (отказ) цветом.
в) Выполнить проверку работоспособности передающей системы в следующем порядке:
– выбрать режим "Работа F3" и установить следующие команды управления "ПОДРЕЖИМ РАБОТЫ" – "ДЕЖ", "ВЫСОКОЕ" – "ВКЛ", "НАГРУЗКА" – "ЭКВ";
– нажать кнопку "ВВОД";
– перейти в режим "Технологический F4" и на вкладке "САУ (F4)" установить флажок "Отключить фоновую калибровку", подтвердить команду нажатием кнопки "ВВОД";
– перейти в режим "Контроль F1" и в панели "Контроль ПС" установить следующие параметры: "F, МГц" (установить произвольное значение несущей частоты в пределах рабочего диапазона частот изделия), "dAm" – "НЕТ", "dF" – "НЕТ", "M–послед" – "0";
– установить флажок "Включить" и нажать кнопку "Запуск";
– контролировать исправную работу передающей системы по подсвечиванию зеленым цветом индикаторов состояния "УМП выход", "УМВ выход";
– завершить проверку снятием флажка "Включить" и нажатием кнопки "Запуск".

ПЕРЕЗАПУСК И ЗАВЕРШЕНИЕ РАБОТЫ

Для перезапуска функционального программного обеспечения АРМ1 (АРМ2) и завершения его работы необходимо перейти на главную ЭФ и нажать на кнопку "Выход (F12)". При этом появится окно "Завершение работы" с переключателями выбора функций: "Перезапустить АРМ" и "Завершить работу АРМ", а также кнопками "ОК" и "Отмена".

Для перезапуска АРМ1 (АРМ2) необходимо:
1) выбрать функцию "Перезапустить АРМ";
2) нажать кнопку "ОК".

Для завершения работы АРМ1 (АРМ2) необходимо:
1) выбрать функцию "Завершить работу АРМ";
2) нажать кнопку "ОК";
3) дождаться появления на экране сообщения "System halted –";
4) на ПУ ЭВМ АРМ1, АРМ2 тумблер "ПИТАНИЕ – ОТКЛ" перевести в положение "ОТКЛ".

ВНИМАНИЕ !

Запрещается работать с открытыми дверьми машины при включенном перератиде !

Introduction

Russia's conventional military capabilities have become the subject of much speculation and analysis in recent years, partly in response to its military operations but also due to its ambitious military modernisation programme and consistent state funding for this process. This interest has more recently extended beyond media, academic and professional military levels into national government and NATO efforts to appreciate better the actual capabilities of Russia's Armed Forces, mainly driven by the deterioration in Russia's relations with the US and NATO following the annexation of Crimea in 2014 and the ensuing Ukraine crisis. While Russia's capability matrix is growing and is difficult to measure from a foreign perspective, these efforts are frequently two-dimensional or mechanical, which may stem from a lack of awareness of the history of and developments in Russian military thinking and theory, with particular reference to the General Staff's interest in "force multipliers" in the context of possibly confronting potentially high-technology adversaries.

This study therefore attempts to reference these factors to examine how and why Russia's military has turned its attention since the reform initiated in late 2008 to more fully exploiting and developing significant use of the electromagnetic spectrum (EMS) by employing electronic warfare assets. This is consistent with the interest in adopting network-centric approaches to military operations as the Russian military becomes further informationised, as well as the aforementioned "force multiplier" interests. The study seeks to avoid exaggeration of the threat this may pose to the Alliance or its members, concentrating on the evolution and continuance of this effort to bolster electronic warfare (EW) capability.

Consequently, the report is divided into three parts. It seeks to place Russia's Armed Forces' EW capability in the context of its wider military capabilities, examining the organisational structure of these forces and their historical and possible future development. It shows, for example, how the EW forces are represented throughout Russia's Armed Forces from strategic to tactical levels, and the advocacy for these forces within the military and defence industry. In the second chapter, the modernisation of the EW systems and equipment in Russia's Armed Forces is considered, after debunking the wilder media-based claims concerning the possibility that the Russian military already possesses the capability to exploit EW to "switch off" NATO systems and force Alliance troops to fight in a technology-denied operational environment.

In the final chapter, the practical implications of these advances are considered by providing an overview of Russia's EW usage in recent conflicts, from Chechnya to Ukraine. Finally, some conclusions are drawn from the study in relation to what these advances might mean for NATO and its defence planning, especially linked to bolstering defence and deterrence on its Eastern Flank. The report concludes that Russia's EW capability, as it expands further, will compel an adjustment in NATO training and efforts to reinforce its eastern members, in recognition that any future conflict between Russian and Alliance forces would be fought in an EMS-contested battlespace.

This study seeks to examine the evolution and likely future interest of the Russian military in EW capability by using almost exclusively Russian specialist and military literature and sources. This has been refined by research interviews with EW specialists, and experts and practitioners with knowledge of the continued conflict in south-eastern Ukraine. Its overall purpose is to inform the policy community and planning staffs about the underlying drivers involved in Russia's EW capability and the implications this may carry, and to plug a gap in the analytical coverage of Russian defence and security studies, which has overlooked or underestimated the EW dimension to its military modernisation.

1. EW as Part of Wider Capability

1.1 Russia's Military Thought about EW

Russia's electronic warfare (*radioelektronnaya bor'ba*—REB) capability has evolved in recent years into a formidable combat support asset, which forms a key part of its overall conventional Armed Forces.[1] To understand the context of this development, it is necessary to examine how this fits into Russian military capability, particularly referencing the General Staff's well-known and long-standing interests in developing "force multipliers" to compensate for comparative weaknesses in the event of combat against a high-technology opponent.[2]

Indeed, Russia's military capability and how this may be enhanced in the future cannot be simplified into measuring the various arms and branches of its services, examining weapons and equipment advances etc.; nor can its weakness compared to NATO be taken at face value.[3] In the case of the latter, conflict scenarios are more likely on Russia's periphery where its Armed Forces already hold several potentially critical advantages related to geography, location, logistics and speed of moving forces into position, as well as other local factors, which would present the Alliance with considerable challenges if fighting were to erupt in NATO's east.

1. D. Dobykin, A.I. Kupriyanov, V.G. Ponomarev and L.N. Shustov, *Radioelektronnaya bor'ba. Silovoe porazhenie radioelektronnykh sistem* [Electronic warfare. Kinetic strikes on electronic systems] (Moscow: Vuzovskaya kniga, 2007); A.I. Paliy, *Ocherki istorii radioelektronnoi bor'by* [Essays on the history of electronic warfare] (Moscow: Vuzovskaya kniga, 2006); V.G. Radziyevskiy, *Sovremennaya radioelektronnaya bor'ba. Voprosy metodologii* [Contemporary electronic warfare. Issues of methodology] (Moscow: Radiotekhnika, 2006); V.V. Tsvetnov, V.P. Demin and A.I. Kupriyanov, *Radioelektronnaya bor'ba. Radiomaskirovka i pomekhozashchita* [Electronic warfare. Electronic camouflage and defence against interference] (Moscow: MAI, 1999).
2. A.Nagalin, Y. Donskov and I. Anisimov, "Iyerarkhiya tseley i zadach, vozlagayemykh na podrazdeleniya REB v obshchevoyskovom boyu" [The hierarchy of objectives and tasks given to EW units in combined-arms warfare], *Voyennaya Mysl'* No. 4 (2013): 77–84.
3. V. Baulin and A. Kondratyev, "Realizatsiya kontseptsii 'setetsentricheskaya voyna' v VMS SShA" [Implementation of "network-centric warfare" concept in the US Navy], *Zarubezhnoye Voyennoe Obozreniye*, No. 6, June 2009, http://pentagonus.ru/publ/26-1-0-811 (accessed July 10, 2017).

Likewise, Russia's General Staff has a high level of interest in using "force multipliers" and asymmetric responses in order to try to level the playing field vis-à-vis any high-tech adversary; EW plays a critical role in the pursuit of such "force multipliers", and the level of attention paid to this area in recent years by Russian defence planners has grown markedly.[4] How do senior Russian officers see this capability? How is it defined? Does their understanding of EW differ from that of US and NATO counterparts? In what ways has Moscow sought to strengthen EW capability? To what extent is this integrated into Russia's Armed Forces in training, procurement and doctrine, and what impact might this have on operational capability? Before turning to how EW is understood in the Russian military and exploring the organisational reforms and structure of its EW forces and its longer-term role in the military, more context is needed.

Russia's electronic warfare capability has evolved in recent years into a formidable combat support asset

Since Moscow initiated genuine reform and modernisation of the Armed Forces in 2008, some Russian strategists have been advocating network-centric warfare (*setetsentricheskaya voyna*) as a vital "force multiplier" and a means to instigate deeper and meaningful military transformation; an essential element in this approach involves EW. Its origins, of course, lie in late Soviet and Russian military theory and the proponents of the Revolution in Military Affairs (RMA).[5] This is most visible

4. In January 2012, the then president, Dmitry Medvedev, signed a decree titled *Osnovy politiki Rossiyskoy Federatsii v oblasti razvitiya sistemy radioelektronnoy bor'by na period do 2020 goda i dal'neyshuyu perspektivu* [Fundamentals of the Policy of the Russian Federation in Development of an Electronic Warfare System in the Period up to 2020 and Beyond]; the content appears to be classified.
5. Vasiliy Burenok, "Bazis setetsentricheskih voyn–operezhenie, intellekt, innovatsii" [The basis of network-centric wars—advance, intellect, innovations], *Nezavisimoye Voyennoe Obozreniye,* April 2, 2010, http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html (accessed July 10, 2017); Vasiliy Burenok, Alexey Kravchenko and Sergey Smirnov, "Kurs–na setetsentrcheskuyu sistemu vooruzheniya" [The course set towards network-centric system of armaments], *Vozdushno-Kosmicheskaya Oborona*, May 2009, http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya (accessed July 10, 2017).

in Moscow's concerted efforts to streamline command and control (C2), to design and procure automated C2 systems throughout its Armed Forces, and to change some of its approaches to warfare. What changed during the past decade is that the Russian political-military leadership has acted on these theoretical approaches to future warfare, becoming more open to alternative perspectives on how information is transforming the battlespace, consequently investing in the necessary modernisation programme. As the Commander of Russia's EW Forces, Major-General Yuriy Lastochkin, noted:

> *There is nothing surprising that in the current circumstances, EW—as a relatively inexpensive and easily implemented means to disrupt the functioning of an enemy's radar and other systems and to defend one's own similar systems from interference—is emerging as a priority and a focus for development. In certain circumstances, use of EW approaches can be viewed as asymmetric measures that negate the benefits of an adversary's highly sophisticated systems and means of armed combat.*[6]

Indeed, Russian military theorists and planners have well-established interests in analysing and assessing trends in future warfare and in trying to promote new capabilities. These views and discussions lead into numerous areas, but there are also some common themes.[7] Existing military modernisation plans draw upon such ideas, with reference to robotics and nanotechnologies and even to further developing or refining the "non-military means" elements in the Russian hard/soft power mix. However, Moscow has placed C4ISR capability and enabling the Armed Forces to introduce network-centric approaches to warfare at the very epicentre of its transformation and modernisation drive since 2008–9.[8] It is a unifying theme in the transformation, underpins the defence industry's support for modernisation, and guides and shapes experimentation with force structure, manpower and the application of platform-based operations in an informationised combat environment.

Moscow has placed C4ISR capability and network-centric approaches to warfare at the very epicentre of its transformation and modernisation drive

According to an official definition in *Voyennyy Entsiklopedicheskiy Slovar'* ("Military Encyclopedic Dictionary"), *radioelektronnaya bor'ba* (electronic warfare) is a type of armed struggle using electronic means against enemy C4ISR to "change the quality of information", or using electronic means against various assets to change the conditions of the operational environment. EW consists of suppression and protection (see Annex A). It aims to "reduce the effectiveness" of enemy forces, including command and control and their use of weapons systems, and targets enemy communications and reconnaissance by changing the "quality and speed" of information processes. In reverse, EW in defence protects such assets and those of friendly forces.[9]

It is very important to grasp this definition and how it is understood in the Russian military hierarchy. EW could be seen either as representing a cluster of activities to gather intelligence and target enemy radio and electronic assets and provide protection to friendly forces, or as denoting warfare in the sphere of information systems (see Annex A). Yet even the official definition from 2007 falls short of how Russian military theorists and

6. Viktor Khudoleev, "Voyska dlya srazheniya v efire" [Troops for combat on airwaves], *Krasnaya* Zvezda, April 14, 2014, www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire (accessed July 10, 2017).
7. Olga Bozhyeva, "Festival' 'novaya voyna'" [Festival "New War"], *Moskovskiy Komsomolets,* October 17, 2009, http://www.mk.ru/editions/daily/article/2009/10/08/364473-festival-novaya-voyna.html (accessed July 10, 2017).
8. Andrey Garavskiy, "Svyaz' reshaet vse" [Communications determine everything], *Krasnaya Zvezda,* June 4, 2010, http://old.redstar.ru/2010/05/22_05/1_01.html (accessed July 10, 2017).
9. "Voyennyy Entsiklopedicheskiy Slovar'" [Military Encyclopaedic Dictionary], *Ministerstvo Oborony Rossiyskoy Federatsii,* accessed May 19, 2017, http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14416@morfDictionary.

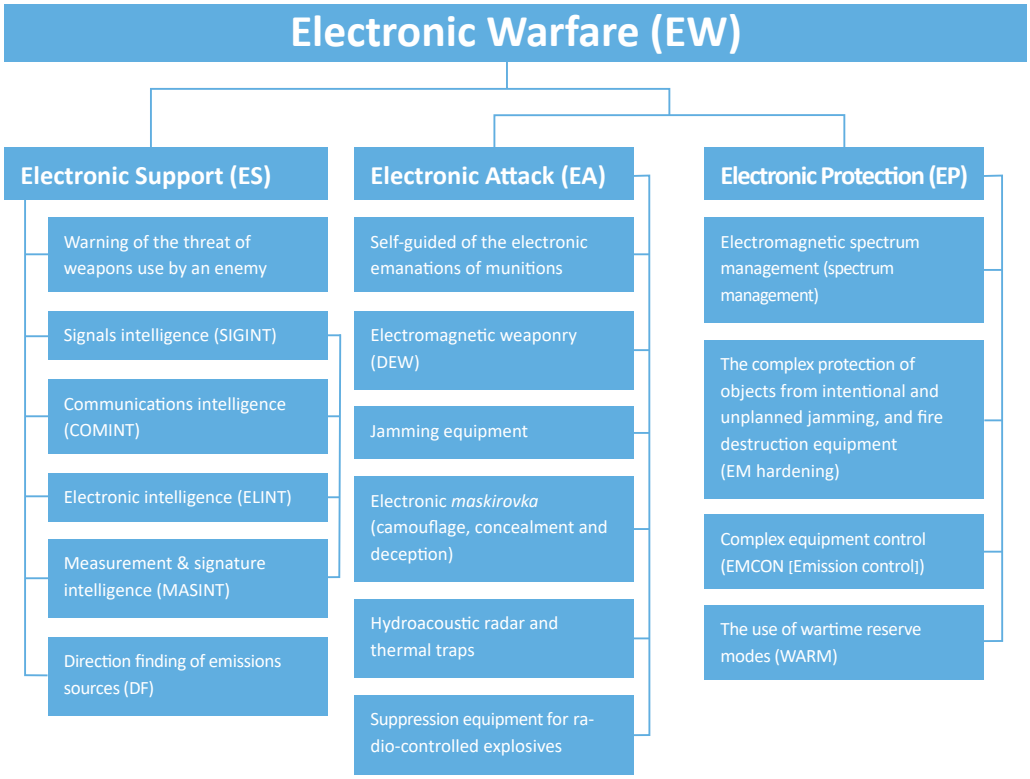


Figure 1: Electronic Warfare (EW)[12]

specialists use the term now. One independent Moscow study frames the scope of EW more narrowly, as restricted to the "radio wave spectrum", despite abundant evidence that Russian military top brass and theorists see this as functioning in the EMS.[10]

Indeed the term *radioelektronnaya bor'ba* would be more literally translated as "radio-electronic combat [or struggle]" and reflects the origin of the phrase in the early 20th century during Russia's operations against Japan and the need to monitor and disrupt radio signals.[11] The use of *radioelektronnaya bor'ba* in contemporary Russian military discussion acknowledges a transition to the modern information environment, and one in which its military will operate in the EMS, and this evidently extends well beyond a narrower definition of operating in radio wavelengths. The primary targets for EW forces are, therefore, radio and cellular communications, radar, and enemy electronic systems and EW capability. Consequently, EW suppresses or protects—depending on whether for attack or defence—the following targets:

- C4ISR;
- location and target distribution systems;
- fire control;
- computers;
- utility/network systems.

Moreover, before anything can be suppressed, it first has to be intercepted. This depends on the success of Signals Intelligence (SIGINT) through Electronic Intelligence (ELINT) or Communications Intelligence (COMINT)—intelligence received through Electronic Support (ES). When it is identified it can be suppressed, neutralised or destroyed by means of targeted Electronic Attack (EA). To defend these systems, Electronic Protection (EP) is employed. The point here is to underscore for the reader how interconnected EW is with other technical intelligence assets functioning in the EMS (see Figure 1). It is also worth noting the symbiotic relationship between EW and cyber-warfare, though the latter lies beyond the scope of this report; as in China, it is highly likely that Russian

10. N.A. Kolesova and G. Nasenkova (eds.), *Radioelektronnaya bor'ba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego* [Electronic Warfare. From the Experiments of the Past to the Future Decisive Front] (Moscow: CAST, 2015), 14–42.
11. A.I. Paliy, "Radioelektronnaya bor'ba v khode voyny" [Electronic warfare in the course of war], *Voyenno-Istoricheskiy Zhurnal* No. 5 (1976): 10–16.

EW and cyber-warfare capabilities will merge. Cyber-warfare is about managing the challenges in free space in the EMS, while EW is about non-free space.[13]

A comparison of EW in Russian and US or NATO militaries is problematic not least because in Russia's Armed Forces there is no concept of war fighting functions (WFF). Equally, in the Russian context there is a different military decision-making process in play. Also, as already noted, there is a close relationship between SIGINT and EW, and in the Russian military EW units also perform an additional SIGINT function. There also appears to be a close link between SIGINT, air defence, artillery and EW, which is evident in Russia's application of hard power in south-eastern Ukraine.[14] Russian EW units are tasked with the protection of artillery from enemy targeting, and act in close coordination with SIGINT to cue action by either air defence or artillery units. Tactical Russian EW systems are used in artillery targeting. To better understand these issues and the centrality of EW in Russian military operations, it is necessary to outline the organisational structure of Russia's EW forces.

There appears to be a close link between SIGINT, air defence, artillery and EW, which is evident in Russia's application of hard power in south-eastern Ukraine

1.2 Organisational Structure of Russia's EW Forces and Industry

As a result of the reform of Russia's Armed Forces initiated in late 2008, moving from a divisional and largely "cadre" system to fuller manning in a brigade-based system, the manoeuvre brigades (tank and motorised rifle) were restructured to contain an EW unit in their organic structure (see Figure 2). In the top section of the diagram can be seen the set of battalions in the Motorised Rifle Brigade (MRB), with the combat support elements lower left and the combat service support such as logistics at lower right; among the combat support units is the EW Company (structure shown in Figure 3). The EW systems located in the Ground Forces' manoeuvre brigades, which include MRBs and tank brigades, provide coverage of up to 50 km.

This is a salient feature of Russian Ground Forces as, unlike their Western counterparts, the EW component is represented organically within the brigade structure, which means that the Russian Ground Forces do not move or conduct operations without EW support. At this level the EW assets are tactical, although EW Forces are present throughout Russia's Armed Forces—in the Ground Forces, Airborne Forces (*Vozdushno-Desantnye Voyska*—VDV), Aerospace Forces *(Vozdushno-Kosmicheskiye Sily*—VKS) and Naval Infantry—and are involved in the Navy and the Strategic Rocket Forces (*Raketnyye Voyska Strategicheskogo Naznacheniya*—RVSN). The Ground Forces are the main advocate of EW in the Russian military. General Lastochkin outlines the EW forces as follows:

Russian Ground Forces do not move or conduct operations without EW support

> *EW forces and means are part of the strategic system of radio jamming, Integrated Technical Control* (kompleksny tekhnicheskiy kontrol'—KTK)*, and the array of EW units of military districts, large formations [armies] and formations [divisions, brigades] of the services and branches of the RF Armed Forces.*[15] *At present, the main forces and means are concentrated in the Ground*

12. Maksim Shepovalenko, "Boevye lazery budushchikh voyn" [Combat lasers of future wars], *Voyenno-Promyshlennyy Kuryer*, July 3, 2013, http://www.vpk-news.ru/articles/16579 (accessed July 10, 2017).
13. EW specialists use this distinction to differentiate between the propagation of EM waves in an open environment and that constrained by physical boundaries such as optical cables and electronics.
14. V. Silyuntsev, V. Demin and D. Prokhorov, "Boyevoye primeneniye REB" [Combat application of EW], *Armeyskiy Sbornik* No.7 (2016): 43–53, accessed July 10, 2017, http://sc.mil.ru/files/morf/military/archive/AC_07_2016.pdf
15. KTK seems to be a Russian variant of Electronic Support.

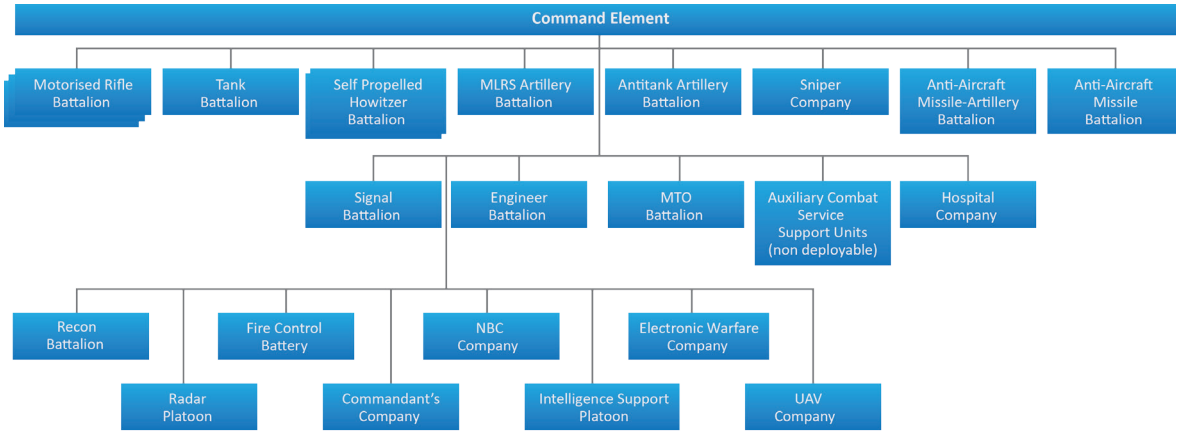


Figure 2: Motorised Rifle Brigade structure

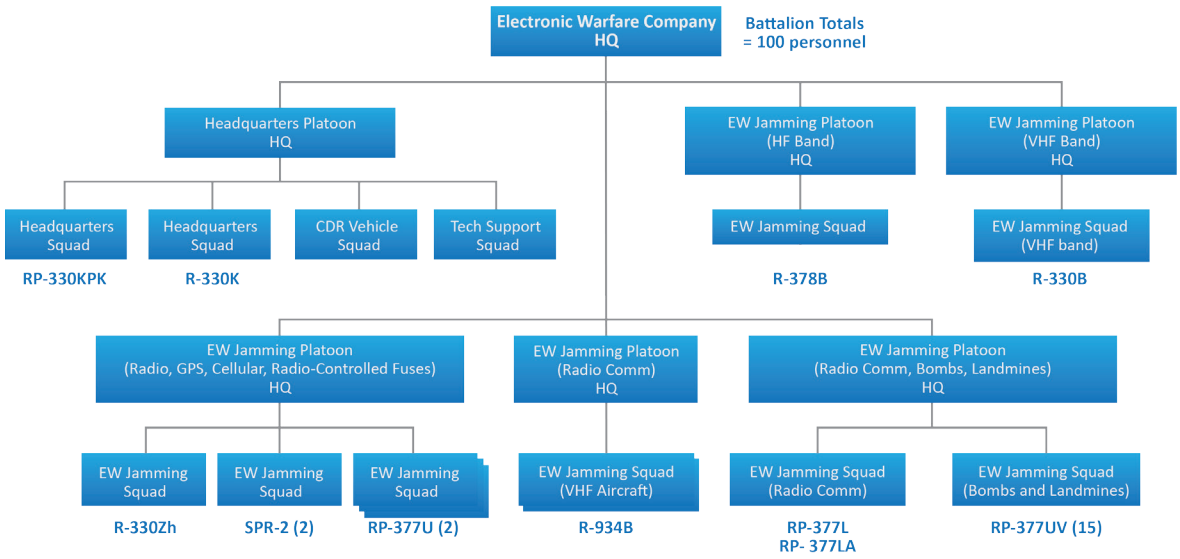
> *Troops, Aerospace Forces and Navy, and the component inter-service groupings of military districts. In the VDV, we've established EW sub-units in assault divisions. In the RVSN, there are KTK sub-units for every missile Ground Forces, division, and testing ground. Since 2014, the forces and means of radio jamming in the districts have carried out duty missions.*[16]

Alongside the restructuring of the Armed Forces in 2008–9 and the reform of the system of military districts (MDs)/joint strategic commands (*Obyedinyonnoye Strategicheskoye Komandovaniye* – OSK), EW forces experienced a similar transformation. This process saw the move from disparate EW units throughout the military to reorganising them at operational and strategic levels into brigades. In April 2009, in Western MD, the 15th EW Brigade was formed in Novomoskovsk (Tula Oblast), and later transferred to Tula, and the process of forming the additional EW brigades was finally completed by December 2015 with the 19th EW Brigade in Rassvet, Southern MD. As a result, Russia currently has five EW brigades across its MDs, with two located in Western MD (see Figure 4)—though this may well change in the future as demand for EW capacity increases. Each of these brigades consists of four EW battalions and one company.[17] In addition, the EW forces have centres in the naval fleets and battalions in the MDs; the latter are probably tasked with the protection of critical infrastructure. In December 2009, Moscow and Minsk signed a bilateral defence agreement to cooperate on EW and planned to form a unified EW system for the regional group of forces; Belarus appears to be Russia's partner in EW.[18]

The formation of the 15th EW Brigade in April 2009 marked a turning point in signalling the increased role assigned to EW in the Russian military. Although this occurred during the rapid effort to switch the Ground Forces to a brigade-based structure by restructuring existing formations and abolishing "cadre" or paper divisions in 2009, the process of forming the EW brigades has been slow and ponderous by comparison. Forming the fifth EW brigade (the 19th) in late 2015 may not mark the end of that process as EW capacity continues to expand, but it has provided a better-organised

Moscow and Minsk signed a bilateral agreement to cooperate on EW and planned to form a unified EW system for the regional group of forces

16. Yuriy Lastochkin and Oleg Falichev, "Kupol nad Minoborony" [A dome above the Ministry of Defence], *Voyenno-Promyshlennyy Kuryer,* April 26, 2017, http://www.vpk-news.ru/articles/36422 (accessed July 10, 2017).
17. Aleksey Ramm, Dmitriy Litovkin and Yevgeniy Andreyev, "V voyska radioelektronnoy bor'by pridet iskusstvennyy intellekt" [Electronic warfare troops will be joined by artificial intelligence], *Izvestiya*, April 4, 2017, http://izvestia.ru/news/675891 (accessed July 10, 2017).
18. "Moscow, Minsk to jointly prepare electronic warfare structure", *Interfax*, June 8, 2011, http://www.interfax.com/newsinf.asp?id=250211 (accessed July 10, 2017).



Key to EW equipment

RP-330KPK: VHF Automated Command Post; RP-330K: Automated Control Station; R-378B: HF Automated Jamming Station; R330B: VHF Frequency Jammer linked to the *Borisoglebsk*-2 HF Automated Jamming System; R-330Zh: *Zhitel* Automated Jammer against INMARSAT and IRIDIUM satellite communication systems, GSM and GPS; SPR-2: VHF/UHF Radio Jammer; RP-377U: Portable Jammer (against IEDs); RP-934B: VHF Automated Jamming Station against communications and tactical air guidance systems; RP-377L: IED Jammer; RP-377LP: Portable Automated Jammer; RP-377UV: Portable Automated Jammer.

Figure 3: EW Company

support base for EW across strategic to tactical levels.[19] Russia's most powerful EW systems—such as the *Krasukha*, *Leer*-3, *Moskva* and *Murmansk*-BN—are located in the Ground Forces' EW brigades; these systems offer ranges of several hundred kilometres. These brigades are tasked with providing combat support to the manoeuvre brigades, and can be broken down into smaller parts depending on the size of force and type of mission for which it is tasked. Since 2012, the tempo of EW exercises has increased two-fold and in August 2016 exercise *Elektron-2016* was staged—the first of its kind since 1979—involving EW forces from across all service branches and arms.[20]

In August 2016 exercise Elektron-2016 was staged—the first of its kind since 1979—involving EW forces from across all service branches and arms

In 2009 the loose group of domestic defence industry companies working on manufacturing EW systems underwent vertical integration into Radio-Electronic Technologies Concern (*Kontsern Radioelektronnye Tekhnologii*—KRET), which now conducts intensive lobbying and promotion of EW interests within the Russian military. In addition to KRET, Sozvezdiye and the UAV designer Special Technology Centre (*Spetsialnyy Tekhnologicheskiy Tsentr*—STT) work closely with the EW forces. In 2010 the defence industry formed the Scientific-Technical Centre for EW (*Nauchno-Tekhnicheskiy Tsentr Radioelektronnoy Bor'by*—NTT REB) in Voronezh, responsible for Research and

19. "15-ya otdel'naya brigada radioelektronnoy bor'by" [15th separate electronic warfare brigade], Voyskovye Chasti Rossii, accessed July 10, 2017 http://voinskayachast.net/suhoputnie-voyska/specialnie/vch71615; "19-ya otdel'naya brigada radioelektronnoy bor'by" [19th separate electronic warfare brigade], Livejournal, accessed May 19, 2017, http://bmpd.livejournal.com/1852552.html; Aleksey Ramm, "Elektronnaya voyna—mify i pravda (Part 1)" [Electronic warfare—myths and the truth], *Voyenno-Promyshlennyy Kuryer*, September 30, 2015, http://vpk-news.ru/articles/27272 (accessed July 10, 2017).

20. "Spetsialnye ucheniya Elektron-2016 provodyatsya na yuge Rossii" [Special exercise *Elektron*-2016 is conducted in the south of Russia], *Zashchishchat' Rossiyu*, August 19, 2016, https://defendingrussia.ru/a/cpecialnyje_uchenija_elektron2016_prohodjat_na_juge_rossii-6207/ (accessed July 10, 2017).

Figure 4: Russian Federation EW brigades

Development (R&D) on future EW systems.[21] In October 2015, defence minister Sergey Shoygu established the EW Forces Military-Scientific Committee and, shortly afterwards, two scientific-production companies were formed to promote the modernisation of the EW inventory. The quantity and quality of EW systems being procured by Russia's Armed Forces has similarly grown. Equally, the initial reform in 2009 has been supported by transforming the EW educational and training system, which is ongoing and is expected to see the introduction in 2018 of the first simulators to boost training. All units were re-equipped with *Magniy*-REB training complexes, and the defence ministry plans to introduce an Integrated Training and Learning System (*Integrirovannyy Trenazherno-Obuchayushchiy Kompleks*—ITOK), designed to enhance the training of EW specialists.[22]

Two scientific-production companies were formed to promote the modernisation of the EW inventory

1.3 Historical and Future Development of Russia's EW Forces

Seen from the perspective of definition and evolution of EW in the Russian military and recent organisational transformation or changes within the domestic defence industry to support EW, this is clearly an area to which the top brass assigns growing importance. This is consistent with the historical role of EW in the Soviet and Russian militaries, with the more recent surge in attention representing a correction to its neglect in the immediate aftermath of the end of the Cold War and the disintegration of the Soviet Union. Given the history of Russian EW, its well-established credentials and increasingly significant combat support role, especially in relation to military systemology (*voyennaya sistemologiya*),[23] and the capacity of the Armed Forces to target enemy informational systems, EW proponents lobby for its interests within the Russian defence community—which

21. See AO "Nauchno-tekhnicheskiy tsentr radio-eletronnoy bor'by" [JSC Scientific-technical centre for electronic warfare], http://www.ntc-reb.ru/ (accessed July 10, 2017).
22. Yuriy Lastochkin, "Ni dnya bez pomekh" [Not a day without interferences], *Voyenno-Promyshlennyy Kuryer,* April 27, 2016, http://www.vpk-news.ru/articles/30428 (accessed July 10, 2017).
23. This was a new discipline, which relies on modelling and cybernetics to establish a relevant theory of combat systems among other military forecasting techniques. See V.D. Ryabchuk, "Nauka, obrazovaniye, reforma" [Science, education, reform], *Voyennaya mysl'* No. 2 (1994): 39–41; V.D. Ryabchuk et al., *Elementy voyennoy sistemologii primenitel'no k reshenyu problem operativnogo iskusstva i taktiki obshchevoyskovykh ob'edineniy, soyedineniy i chastey: Voyenno-teoreticheskiy trud* [Elements of military system applicable to solving problems of operational art and tactics of combined-arms formations and units: Military-theoretical work] (Moscow: Izdatel'stvo Akademii, 1995).

weighs against its younger siblings, information warfare and cyber-warfare. Here the history is important, as it shows the Russian EW Forces as well established, credible and in pole position for high-end financial support from the state. Tracing an outline of the future role of EW in the Russian Armed Forces' priorities requires reference to the views of the Russian expert community and its leading EW theorists, and how the EW leadership perceives the growth of this combat service.

EW proponents lobby for its interests within the Russian defence community—which weighs against its younger siblings, information warfare and cyber-warfare

Russia's electronic warfare forces trace their roots to 1904 and the defence of Port Arthur against Japan. The need for EW stemmed from the development of using telegraph signals in warfare in the previous century. Soviet EW forces were important elements in the major battles of the Second World War and in the use of radio-detonated mines in Kyiv, Odessa, Orsha and Kharkiv.[24] By 1956, the Soviet Union had activated its first communications, radar and radio-navigation jamming battalions in all branches of the Armed Forces.[25] And by the 1970s, Soviet EW had matured into a higher-level combat support capability, evolving from its earlier role in occasional supporting events such as jamming enemy radar to form an organic EW force to suppress enemy electronic assets and systems in operations or engagements.[26]

Russia's interests in the area of EW received a significant boost from its analysis in the 1990s of the use of EW by the USA and its coalition partners in the First Gulf War in 1991. In many of the studies by Russian General Staff officers in the 1990s, the EW usage by the US military in 1991 is a recurring theme. Jacob W. Kipp observed this in 1997, and in the late 1990s leading Russian military theorists were paying attention to the role of EW as a "force multiplier" long before EW came to be viewed this way in official defence circles in Moscow.[27] As Russian military theorists and defence scholars grappled with the development of network-centric warfare and C4ISR integration in foreign militaries, the role played by EW was never far from their thinking.[28]

In fact, a uniting theme among the expert Russian military community, defence scholars and military theorists and present EW leadership is the extent to which they see future synergy between EW and network-centric warfare capability. There are other unifying themes, but

A uniting theme among the expert Russian military community is the extent to which they see future synergy between EW and network-centric warfare capability

in the first instance the views of Russian experts on the future role of EW in Russia's Armed Forces can be summarised as follows:

- The integration of EW assets and systems into the unified automated C2 system; here it is understood that the role played by EW in network-centric operation is large and

24. Sergey Kozhevnikov, "Radioelektronnaya bor'ba v gody Velikoy Otechestvennoy voyny" [Electronic warfare during the years of Great Patriotic war], *Belorusskaya Voyennaya Gazeta*, April 16, 2014, https://vsr.mil.by/2014/04/16/radioelektronnaya-borba-v-gody-velikoj-otechestvennoj-vojny/ (accessed July 10, 2017).
25. Dobykin, et al, *Radioelektronnaya bor'ba. Silovoe porazhenie*; Paliy, *Ocherki istorii*.
26. Tsvetnov et al, *Radioelektronnaya bor'ba. Radiomaskirovka*; V.V. Tsvetnov, V.P. Demin and A.I. Kupriyanov, *Radioelektronnaya bor'ba. Radiorazvedka i radioprotivodeystviye* [Electronic warfare. Electronic intelligence and electronic counter-measures] (Moscow: MAI, 1998).
27. Jacob W. Kipp, "Confronting the RMA in Russia", *Military Review* 77(3) (1997): 49–55, accessed July 10, 2017, http://fmso.leavenworth.army.mil/documents/confront.htm.
28. E. Kruglov, 'Perspektivy razvitiya amerikanskikh sredtsv REB i taktika ikh primeneniya v sovremennykh vooruzhonnykh konfliktakh' [Prospects of development of the American EW means and tactics of their employment in contemporary armed conflicts], *Zarubezhnoye Voyennoye Obozreniye* No. 2 (2014): 57–63, accessed July 10, 2017, http://pentagonus.ru/publ/perspektivy_razvitija_amerikanskikh_aviacionnykh_sredstv_rehb_i_taktika_ikh_primenenija_v_sovremennykh_vooruzhjonnykh_konfliktakh_2014/18-1-0-2480.

likely to grow, with cyber-warfare playing a secondary supporting role;

- Unifying EW systems with Identification Friend or Foe (IFF) systems, which will involve further integration of Russian EW systems and its high-precision weapons systems deployed in theatres of operations;
- Improvement of the component base to develop future EW systems, especially in overcoming the issue of systems compatibility (EW that might interfere with Russian or friendly systems);
- Developing radio-photon technology in order to lay the basis for a new generation of EW systems.[29]

Many of these observations are reflected in the work of Russian military theorists, but the latter take the EW role still further. In a September 2016 article written by a group of Russian military EW specialists in the theoretical journal of the General Staff, *Voyyennaya Mysl'* ("Military Thought"), the evolution of EW was placed in context and the authors argued that in future EW would transform into a discrete arm of service; this would mean it moved from a support role to a fully-fledged combat arm. Korolyov, Kozlitin and Nikitin note:

> *The first decade of the 21st century was marked by several factors that indirectly influenced not only the EW forces and assets composition and place in operations, but also their combat use methods, accordingly. The first factor is related to a qualitatively new material base for the information support to the troop command and control. Passing to network-centric information support for combat actions, including that for the troop command and control, realized by the leading foreign armies, together with forming Common EW Information and Communications Environment, based on these principles, not only significantly complicated the conditions for combatting the adversary's radio communication system and information-driven assets, but also revealed an inadequacy in existing approaches to disorganizing the troop command and control.*[30]

By 2025 or later, the EW Forces could emerge as a new combat arm with a pivotal role in military operations

Korolyov, Kozlitin and Nikitin highlight the growing role of EW in Russian operations, its transformative character and its potential to contribute to shaping the battlespace in an information era to argue that it may deserve more funding and elevation to a combat role in its own right. In the view of these authors, as shown in Figure 5, since 2015 the EW Forces *de facto* play this part in Russian operations. Quite striking is the extent to which they see EW as playing more than a supporting role; if correct, and with greater state funding, by 2025 or later, the EW Forces could emerge as a new combat arm with a pivotal role in military operations. Should this occur, it would certainly prove consistent with Russian military thinking on exploiting "force multipliers".

What is most relevant from the work of these authors, as outlined in the diagram, is the exponential growth of EW and the role it plays in modern warfare, from its earliest origins through to the 21st century. More striking still, noting the right side of the diagram, the authors place EW not in a narrow field of functioning against enemy radio communications, but in the much broader EMS. It is significant, more than any public statements or rhetoric, that Russia's military theorists recognise the EMS as another legitimate domain of warfare, in addition to land, air, sea and space. Moreover, such theorists are not alone as advocates of a greater future role for the EW Forces.[32]

Consistent with these views among Russian experts and military theorists, General

29. Kolesova and Nasenkova, *Radioelektronnaya bor'ba*, op. cit.: 230–8.
30. I. Korolyov, S. Kozlitin and O. Nikitin, "Problemy opredeleniya sposobov boevogo primeneniya sil i sredstv radioelektronnoy bor'by" [Problems of determining ways of employing forces and means of electronic warfare], *Voyennaya Mysl'* No. 9 (2016): 14–19.
31. Korolyov, Kozlitin and Nikitin, "Problemy opredeleniya sposobov boevogo primeneniya", op. cit.
32. Yuriy Lastochkin, "Rol' i mesto radioelektronnoy bor'by v sovremennykh i budushchikh boyevykh deystviyakh" [Role and place of electronic warfare in contemporary and future combat actions], *Voyenayya Mysl'* No. 12 (2015): 14–19.

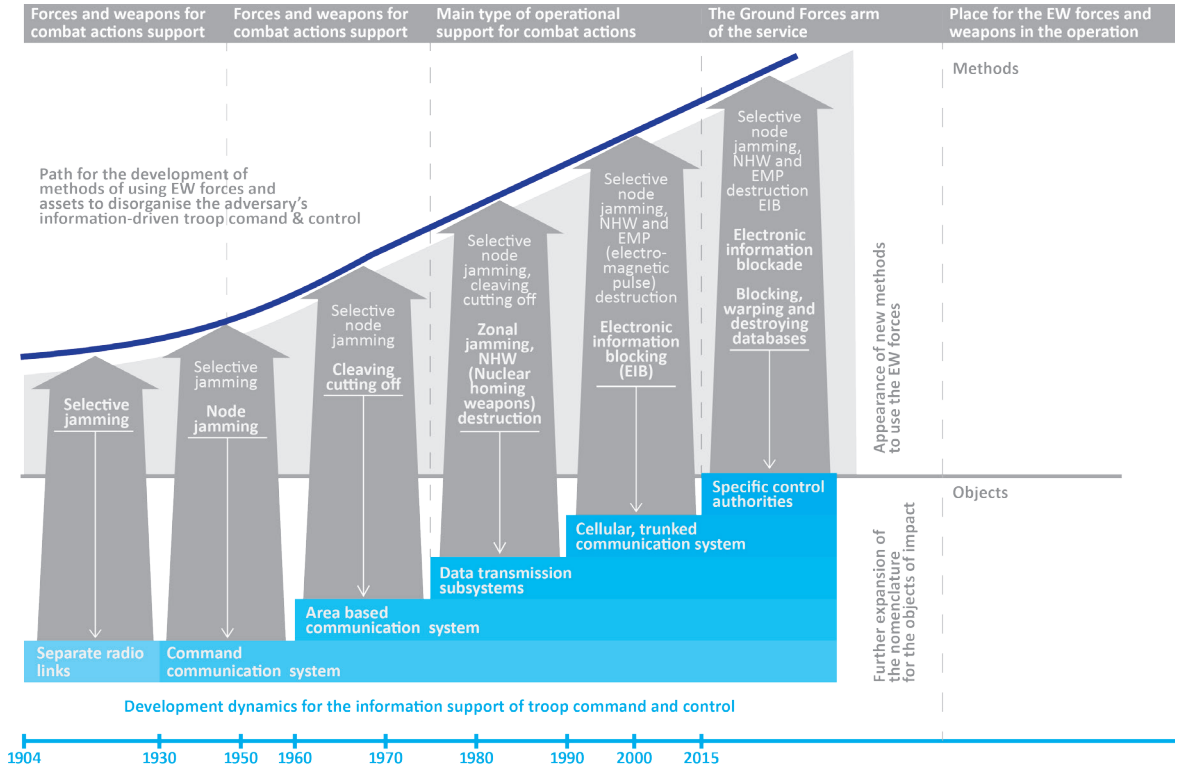


Figure 5: EW disorganising enemy command and control[31]

Lastochkin similarly sees a bright future for the EW Forces, and outlines their major development priorities as focused in these areas:

- Deployment of controlled fields of radio suppression on enemy territory on the basis of unified small-dimension reconnaissance and jamming modules delivered by UAVs;
- Creation of defeat means with powerful electromagnetic radiation on the basis of the employment of specialised munitions and mobile systems;
- Development of programmable equipment for action on highly-organised command and control systems by destroying the accessibility, integrity and confidentiality of information;
- Introduction of means of imitating a false electronic situation and disinforming the enemy's system of troop C2 and weaponry;
- Increasing the level of information security of points of EW C2, improving decision-making support algorithms through the unified circuit of command and control of forces and means.[33]

Thus, it is clear that the Russian military has moved well beyond theoretical discussion and analyses of EW in modern warfare to implementing structural change within the Armed Forces and extending the importance and combat support role played by the EW Forces. The extent to which this might have implications for NATO, including strengthening security on NATO's Eastern Flank, can only be determined by carefully examining the advances in Russian EW systems and procurement alongside the growing role assigned to EW in Russian military operations.

2. Russia's Military Modernisation and EW Assets to 2025

Russia's EW Forces have been undergoing an intensive and unprecedented modernisation and re-equipment programme in recent years, and this is set to continue in the State Armaments Programme (*Gosudarstvennaya Programma Vooruzheniya*—GPV) to 2025, with EW playing an increasingly important role in Russian defence planning. While this is providing highly credible systems for the EW Forces, some media reports have tended to

33. Lastochkin, "Rol' i mesto", op. cit.

exaggerate the extent to which such systems could be used to cripple NATO systems. Before outlining the modernisation of these forces and the procurement of advanced EW systems in Western Military District (MD), it is therefore crucial to examine and rebut Russian claims concerning its capability.

Russia's military theorists recognise the EMS as another legitimate domain of warfare, in addition to land, air, sea and space

2.1 Russian EW Mythology

Attention devoted to the issue of Russian EW capability has been influenced by non-specialist commentary in mainstream media surrounding a classic example of Russia running a fake news story. It is necessary to debunk this myth, and show it to be flawed, before considering the actual procurement and progress being made in introducing more modern EW systems in Russia's military. The story relates to a claim that Russian EW "blinded" the *Aegis* ballistic missile defence system on board a US Navy warship in the Black Sea in April 2014.[34]

The facts surrounding the case are that on 10 April 2014, the USS *Donald Cook* entered the Black Sea on a routine patrol mission, and exited 14 days later. On 15 April, coinciding with Russia's EW Day (a public holiday dedicated to EW troops), Russian state-controlled TV channel *Rossiya*-1's news programme *Vesti* ("News") broadcast a story concerning an Su-24 approaching the USS *Donald Cook* on 12 April; US defence officials later confirmed some flypasts by an Su-24. However, in the original *Vesti* broadcast the claim was made that *Khibiny* EW was carried on board the Su-24 and that it succeeded in "switching off" all the systems on the USS *Donald Cook*, including the *Aegis* system.[35]

The Russian media began circulating this narrative and it was soon picked up by multiple Western media sources. The Russian state newspaper *Rossiyskaya Gazeta* re-ran the story on 30 April 2014, and it resurfaced in various forms later in that year. It claimed the Su-24 "closed" with the destroyer and, using the *Khibiny* EW system suspended from its underbelly, turned off the USS *Donald Cook*'s "radar, combat control circuits, and data transmission system". The story was intended to go viral and carry influence, and by June 2017 a Google search for "Donald Cook electronic warfare" (Дональд Кук РЭБ) yielded 16,000 results.

The author has, in fact, frequently been asked by NATO experts and officers whether Moscow has the capability to use EW assets to "blind" Alliance forces in this way. There are a number of key points to make in exposing the fake news story and identifying the weaknesses of the mythology that the *Khibiny* system can "switch off" Aegis:

- The narrative was first used and promoted in Kremlin-linked state media publications, and its placement and other factors such as blogging and trolling activity suggest this was part of a Russian information warfare (IW) campaign;
- In July 2015, the Russian blogger Leonid Kaganov alleged that the Moscow mint had issued 5,000 commemorative medals, each costing 1,000 rubles, about the Su-24's exploits with the USS *Donald Cook*; on the reverse is inscribed the message "*Urok Mira*" ("Lesson of Peace");
- Russian media articles commonly reflect the successes and triumphs of the EW defence industry organisation KRET, and this story and the mythology that grew up around the reporting of the April 2014 incident has certainly promoted KRET's reputation;
- The main Russian narrative concerning the *Khibiny*'s capability fails to mention that the system was actually designed exclusively for use on the new Su-34 platform and the Su-35S and Su-30SM—and not an Su-24;

34. "Navy responds to claim ship was scared off by Russian jets with video", *Foxtrotalpha*, June 1, 2015, http://foxtrotalpha.jalopnik.com/navy-responds-to-claim-ship-was-scared-off-by-russian-j-1708178476 (accessed July 10, 2017).
35. This claim was still being advanced by *Vesti* in April 2017: "Electronic warfare: How to neutralize the enemy without a single shot", *Vesti*, April, 17, 2017, http://www.vesti.ru/doc.html?id=2878732&cid=4441 (accessed July 10, 2017).

- Almost exactly two years after the incident in the Black Sea, in April 2016, the USS *Donald Cook* was subjected to similar harassment, this time occurring in the Baltic Sea. Although the Su-24 platform was used to conduct a simulated attack posture during repeated low flights in the vicinity of the vessel, there was no repetition of the previous claim that an EW attack was conducted.[36]

In May 2017, the Atlantic Council's Digital Forensic Research Lab published a debunking of the story along similar lines, tracing in particular how the fake news story was spread including using social media and "inventing" a fake US sailor writing in that medium.[37] Moreover, Russian defence experts also highlighted the incredible nature of the claims concerning the Su-24 and the *Khibiny* EW system, noting that it was designed for use under the Su-34, Su-35S and Su-30SM as they also carry a variant of this system.[38] Some NATO EW specialists also explained to the author the completely unscientific nature of the wild claims. To cap it all, if any doubt remained, in January 2016 even KRET issued its own denial about the "attack" on the USS *Donald Cook*.[39] This example, though apparently isolated, actually appears commonplace in both Russian and Western coverage of Russia's EW systems, especially following Moscow's decision to deploy forces to Syria.[40]

2.2 EW Modernisation Targets and Defence Industry Challenges

EW procurement trends are not only marked by introducing modern systems that are faster with increased ranges—there are other key trends that should prove to be of concern to NATO. These are automation, integration with automated C2 systems, and an overall emphasis upon the disruption of enemy C4ISR. These systems are also becoming more mobile.[41]

Procurement of new EW systems for Russia's Armed Forces was rooted in lessons drawn from its conflicts in Chechnya. This centred on integrating reconnaissance, fire damage and jamming to target the EW system in use by enemy groups there. Combat missions in the North Caucasus accumulated a wealth of experience in using EW in such operations and this in turn pushed technological development, but it was some time before the Russian military really benefited from intensified procurement.

Following the Russo–Georgian War in August 2008, Moscow launched its ambitious reform of the Armed Forces and the new GPV 2011–20 committed to achieving a target of 70% new or modern content in the military inventory.[42] The first period of intense testing and procurement of EW systems was in 2010–13. According to General Lastochkin, in this period state tests were completed and numerous systems were subsequently procured. Among these were *Borisoglebsk*-2, *Alurgit*, *Infauna*, *Krasukha*-2-O, *Krasukha*-S4, *Moskva*-1, *Parodist*, *Lorandit*-M,

36. Author interviews with NATO EW specialists, Washington DC, June 2017.
37. "Russia's fake 'electronic bomb': How a fake based on a parody spread to the Western mainstream", *Atlantic Council's Digital Forensic Research Lab*, May 9, 2017, https://medium.com/dfrlab/russias-fake-electronic-bomb-4ce9dbbc57f8 (accessed July 10, 2017).
38. Aleksey Ramm, "Elektronnaya voyna—mify i pravda (Part 2)" [Electronic warfare—myths and the truth], *Voyenno-Promyshlennyy Kuryer*, October 6, 2015, http://vpk-news.ru/articles/27410 (accessed July 10, 2017).
39. "REB dlya chaynikov" [EW for dummies], KRET, last modified January 18, 2016, accessed July 10, 2017 http://kret.com/media/news/reb-dlya-chaynikov/.
40. "Russian jamming system blocks all NATO electronics over Syria", *Sputnik*, October 29, 2015, http://in.sputniknews.com/world/20151029/1016211289/russian-jamming-system-syria-nato.html (accessed July 10, 2017); "KRET v 2015 godu peredal Vooruzhennym Silam 9 kompleksov REB Moskva-1" [In 2015, KRET handed over to the Armed Forces 9 complexes of EW *Moskva*-1], *RIA Novosti*, December 25, 2015, http://ria.ru/defense_safety/20151225/1348750286.html (accessed July 10, 2017). The tendency to play up Russian EW systems in the Russian media also metastasises to some Western commentaries. See, for example, Dave Majumdar, "The Russian Military's 5 Next Generation Super Weapons", *The National Interest*, November 8, 2015, http://nationalinterest.org/blog/the-buzz/the-russian-militarys-5-next-generation-super-weapons-14276 (accessed July 10, 2017).
41. Aleksandr Sharkovskiy, "Skromnyy potentsial kompleksa Zaslon-REB" [Modest potential of the complex *Zaslon*-REB], *Nezavisimoye Voyennoye Obozreniye*, April 20, 2017, http://www.ng.ru/armies/2017-04-20/2_6978_zaslon.html (accessed July 10, 2017); Aleksey Ramm, "Razrabotchik sistem REB: Amerikanskiye Tomagavki—slozhnyye tseli" [Developer of EW systems: American *Tomahawks*—difficult targets], *Izvestiya*, April 14, 2017, http://izvestia.ru/news/683822 (accessed July 10, 2017); Oleg Vladykin, "Plashchi-nevidimki dlya tankov, korabley i samoletov" [Invisibility cloaks for tanks, ships and aircraft], *Nezavisimoye Voyennoye Obozreniye*, January 29, 2017, http://www.ng.ru/week/2017-01-29/8_6915_army.html (accessed July 10, 2017).
42. "Sovremennym rossiyskim sredstvam REB pod silu 'vyrubit'' tselyy polk" [Modern Russian EW means are capable of "switching off" an entire regiment], *Voyennoye Obozreniye*, December 10, 2014, https://topwar.ru/64421-sovremennym-rossiyskim-sredstvam-reb-pod-silu-vyrubit-celyy-polk.html (accessed July 10, 2017).

Leer-2, *Leer*-3, *Lesochek*, *Less*, *Magniy*-REB and *Pole*-21 (see Annex B).[43]

The procurement process showed no signs of slowing following the initial period of stepping up the tempo of introducing new systems. In the 2014 State Defence Order, KRET reportedly delivered 60.4 billion rubles (one billion dollars)-worth of systems, including IFF, airborne avionics and other EW equipment. The EW Forces saw the introduction of the *Vitebsk* EW system for Su-25s and for the Ka-52 attack helicopter. In 2014, KRET's sales reportedly increased by 40% year-on-year.[44] Similarly, on 15 April 2017 (EW Troops Day), the target for deliveries was set at 450 units for the year. This would involve all elements of the EW equipment range, aimed at suppressing radio communications, navigation, protection against high-precision weapons, and automated command and control for EW systems. Among the EW systems procured in 2017 were additional *Krasukha*-2-0, *Moskva*-1, *Borisoglebsk*-2, *Svet*-KU, *Rtut'*-BM and *Infauna* (see Annex B).[45]

Combat missions in the North Caucasus accumulated a wealth of experience in using EW in such operations and this in turn pushed technological development

Far from being piecemeal in its approach, the procurement of EW systems was shaped and guided generally by the GPV to 2020 and the 70% target. Specifically, the conceptual approach to upgrade EW systems and infrastructure is set out in a presidential decree signed on 9 January 2012: "The Fundamentals of the Policy of the Russian Federation in Development of an Electronic Warfare System in the Period up to 2020 and Beyond" (*Osnovy politiki Rossiyskoy Federatsiyi v oblasti razvitiya sistemy radioelektronnoy bor'by na period do 2020 goda i dal'neyshuyu perspektivu*). However, it appears that the contents of the decree and thus the conceptual guiding document are classified.[46]

It is important to note, therefore, that the strategy to modernise the EW assets in the military was conceived prior to the Ukraine crisis and the subsequent deterioration in Russian–NATO relations. The bulk of the modernisation to date predates the Ukraine conflict, but there is no doubt that adjustments to EW R&D are being factored into procurement planning based on Russia's experience of conflicts in Ukraine and Syria, which has permitted operational testing of these systems. On this basis it can be expected that R&D projects initiated in 2014 and after and coming to fruition in the years ahead will be more clearly geared towards targeting NATO systems. But since the modernisation concepts are closely guarded secrets, it is only possible to extrapolate some of the key elements in Moscow's approach to modernising the EW inventory from public statements by defence officials and defence industry specialists as well as by referencing some of the identifiable trends in the publicly available information of the specifications of procured systems.

The procurement process showed no signs of slowing following the initial period of stepping up the tempo of introducing new systems

There are some clues in the many statements by the defence ministry and senior EW officers that indicate the modernisation of EW is based on examining how such capability has been exploited by the US and NATO in military

43. Yuriy Lastochkin and Oleg Falichev, "Oruzhiye asimmetrichnogo otveta" [Weapons of asymmetric response], *Voyenno-Promyshlennyy Kuryer,* May 14, 2014, http://vpk-news.ru/articles/20241 (accessed July 10, 2017).
44. Nikolai Novichkov, "Russia receives new Mi-8MTPR-1 electronic warfare helicopters", *Jane's Defence Weekly*, March 4, 2015.
45. "V Vooruzhennykh Silakh Rossiyskoy Federatsii otmechayetsya Den' Spetsialista Po Radioelektronnoy Bor'be" [Russian Federation Armed Forces mark the Day of Electronic Warfare Specialist], *Eurasian Defence,* April 15, 2017, http://eurasian-defence.ru/?q=node/38809 (accessed July 10, 2017).
46. Lastochkin, "Rol' i mesto radioelektronnoy bor'by", op. cit.

operations over the past two decades.[47] There also appears to be some influence based on US Prompt Global Strike and developments in US and NATO high-precision weapons that is pushing the defence ministry to plan for countering these.[48] At the outset, despite the opaque nature of the overall aims of the procurement processes, one statement that stands out is from the leadership of KRET, aware of the underlying drivers behind the need for modern EW systems in Russia's military.

Indeed, by November 2016, the First Deputy General Director of KRET, Vladimir Mikheyev, referred to the "National Strategic EW System" as an "asymmetric response to the network-centric system of combat operations" on the part of the US and NATO. He referenced the *Murmansk*-BN as a key part of the subsystem.[49] The *Murmansk*-BN has a reported range of 5,000 km, is deployed on seven trucks, and monitors activity on airwaves, intercepting enemy signals with a broad jamming capability; it uses 32-metre-high antennas and has been deployed in Crimea. Mikheyev said the creation of the Russian EW strategic system can be called the "implementation of a network-centric defence concept". He is in no doubt that this system aims to target NATO C4ISR:

> Murmansk *complexes are targeted against systems operating in the HF band such as the US HF Global Communications System. This network supports communications among all Pentagon* ***command and control entities and ships and aircraft of the United States and its NATO allies*** *[emphasis added]. Only jam-resistant communications by cable can be a full-fledged replacement of it. Satellite systems do not have sufficient stability and throughput. This means that operation of systems which have entered the coverage area of Russian EW complexes will be* ***substantially hampered*** *[emphasis added].*[50]

The strategy to modernise the EW assets in the military was conceived prior to the Ukraine crisis and the subsequent deterioration in Russian–NATO relations

In this context, the level of development in designing and procuring automated control systems to further strengthen EW capability is striking. In April 2017, reports emerged concerning the RB-109A *Bylina*, a fully autonomous system being designed for automated C2 of EW systems at brigade level. The *Bylina* is also believed to include an artificial intelligence system, as it analyses in real time the situation in a combat area, detects and identifies targets, chooses how to suppress these and then issues the relevant orders to EW forces in the field. Procurement is planned to begin in 2018, with the target of fully outfitting the EW brigades by 2025. The RB-109A is fully autonomous and deploys on five all-terrain trucks with its own self-protection system. It automatically interfaces with battalion and company command posts, senior commanders and individual EW systems. In brigade headquarters (HQ), officers only need to monitor the operation of the automated system, as it selects and identifies its targets within seconds.[51]

Viktor Murakhovskiy, military expert and editor-in-chief of *Arsenal Otechestva* ("Fatherland's Arsenal"), notes that *Bylina* uses artificial intelligence algorithms, automating the most complex processes of operation of EW devices. Murakhovskiy notes:

47. Aleksandr Kudryavtsev, "Tenevyye storony radioelektronnoy bor'by" [Shadowy sides of electronic warfare], *Voyennoye Obozrenye*, December 22, 2013, http://topwar.ru/37601-tenevye-storony-radioelektronnoy-borby.html (accessed July 10, 2017).
48. Lastochkin and Falichev, "Oruzhiye asimmetrichnogo otveta", op. cit.
49. Olga Chernysheva, "Obnaruzheniye i podavleniye" [Detection and suppression], *Na Strazhe Zapolyariya*, December 4, 2015.
50. Anton Valagin, "Strategicheskaya sistema REB podavit svyaz' NATO" [Strategic system of EW will suppress NATO's communications], *Rossiyskaya Gazeta*, November 14, 2016, https://rg.ru/2016/11/14/strategicheskaia-sistema-reb-podavit-sviaz-nato.html (accessed July 10, 2017).
51. Andrey Simonov, Denis Khripushin and Mikhail Chikin, "Perspektivy avtomatizirovannogo upravleniya v soyedineniyakh radioelektronnoy bor'by Vooruzhonnykh Sil Rossiyskoy Federatsii" [Prospects of automated command and control in the formations of electronic warfare of the Armed Forces of the Russian Federation], *Materialy ot voysk radioelektronnoy bor'by VS RF* No. 1 (2017): 38-39, accessed May 12, 2017, https://reb.informost.ru/2017/pdf/1-7.pdf.

> *The* Bylina *offers options based on the configuration of reconnaissance activity and the means employed for the suppression of enemy electronics, and also the sequence of their operation, while taking into account the electronic compatibility with its own communications and radar reconnaissance equipment. This is one of the main tasks in modern military conflict, because a huge number of high-precision weapon guidance systems have to be countered with the use of radar reconnaissance equipment. Therefore, the* Bylina *is also called an automated decision-making support system.*[52]

In 2016, Russian Military Transport Aviation (*Voyenno-Transportnaya Aviatsiya*—VTA) received the first Il-22PP *Porubschik* electronic warfare and reconnaissance aircraft, entering service in the 117th Military Transport Aviation Regiment's EW Aviation Detachment. Its development began in the autumn of 2009, based on the Il-18. The *Porubschik* uses electronic jamming to suppress radars on early warning aircraft, air defence missile systems and UAVs at ranges of tens of kilometres.[53] Colonel (retired) Mikhail Khodarenok, military analyst at *Gazeta.ru*, sees the Il-22PP as a necessity for the military. "At one time, a few more options were considered: AN-140 and AN-158 planes with turbojet engines as well as the Tu-214," Khodarenok explains, adding:

> *However, at the time of the formation of the "defence procurement" in 2009, none of these models were yet fully ready to be equipped with the latest electronic warfare systems. Of course, this is not an ideal solution. However, for lack of a better option, a choice had to be made—either to stay without the EW aircraft, or to mount the equipment on the tested wings.*[54]

There are other examples of recent EW innovation. The *Borisoglebsk*-2 is one of Russia's newest tactical EW systems, and began replacing the R-330 *Mandat* in 2012. *Borisoglebsk*-2 reportedly can suppress twice the frequency bandwidth of its predecessor in the HF and UHF bands, and up to 100 times faster. There are additional reports that it possesses a capability to disrupt mobile satellite communications and radar navigation systems. *Borisoglebsk*-2 is mounted on an MT-LBu amphibious armoured carrier chassis.[55] The *Moskva*-1 automated EW system has a reported range of 400 km. It can reconnoitre targets while in passive mode, enabling EW troops to identify enemy positions without revealing their own location. Igor Nasenkov, First Deputy General Director of KRET, explains:

> *Reconnaissance information collected by the module is forwarded to the command post, which tracks the targets in real time and selects the means of attack for each of them. The system itself "targets" and employs up to nine EW systems under its control, blinding or disorienting enemy radar and blocking the use of high-precision weapons.* Moskva-*1 comprises modern automated equipment combining the functions of reconnaissance and control. They make it possible to enhance substantially the speed and accuracy of response to threats. In this sense the* Moskva-*1 systems will be a kind of "brain" of the entire EW defence system of whole regions, revealing enemy plans and hindering the effective functioning of its combat units.*[56]

Rychag-AV is a radar and sonar jamming system designed for installation in helicopters, ships and airplanes and ground vehicles. It is alleged to be capable of jamming sensor systems at distances of hundreds of kilometres. The *Rychag*-AV uses multi-beam antenna arrays with Digital Radio Frequency Memory (DRFM) technology to jam radiofrequency-based weapon systems. KRET claims the *Rychag*-AV has no equivalent in the world. The first batch

52. Ramm, Litovkin and Andreyev, "V voyska radioelektronnoy bor'by pridet iskusstvennyy intellekt'.
53. Alexey Ramm and Yevgeny Andreyev, "'Letayushchikh Medvedey usilyat 'Porubshchikami'" ["Flying Bears" will be reinforced by *Porubshchik*], *Izvestiya*, March 31, 2016, https://iz.ru/news/674705 (accessed July 10, 2017).
54. Nikolay Litovkin, "Russia receives first Il-22PP *Porubschik* electronic countermeasures planes", *Russia Beyond the Headlines*, November 9, 2016, https://www.rbth.com/defence/2016/11/09/russia-receives-first-il-22pp-porubschik-electronic-countermeasures-planes_646271 (accessed July 10, 2017).
55. Yuriy Gavrilov, "Podrazdeleniya elektronnoy voyny proveli obucheniye v Severnoy Osetii" [Electronic warfare units conducted exercises in South Ossetia], *Rossiyskaya Gazeta*, June 26, 2015.
56. "Russian Armed Forces: *Moskva*-1 Systems Can 'Target' Up To Nine Electronic Warfare Systems", *RIA Novosti*, December 25, 2015.

of three Mi-8MTPR1 helicopter-mounted *Rychag*-AV systems was delivered to the Russian Armed Forces on 4 March 2015.[57]

Despite the challenges facing the domestic defence industry to meet the increased demand for new and modern EW systems, since 2010 a consistent and steady growth has been sustained. Nevertheless, as in the case of much of the military modernisation, it is conducted on the back of Soviet-era technology with money invested to actually produce these systems. If next-generation products are to be procured, the domestic defence industry will have to overcome technical challenges to manufacture them. This will involve improving the component manufacturing base and rising to the challenge stemming from radio-photon technology to develop microwave weapons. KRET has set up a specialist laboratory to conduct such research.[58]

It is clear that the EW leadership is increasingly confident about procurement and expects to exceed its 70% target. In April 2017, General Lastochkin listed the main aspirations for Russian EW development:

> *The entire system of measures of organisational development of EW Troops will substantially increase their contribution to winning superiority in command and control, and in employing weapons. The volume of effectively fulfilled missions in various strategic directions will grow by two–two and a half times and by 2020 will reach 85 percent. This in turn will become the basis of an effective air-ground EW system, capable of neutralising the enemy's technological advantage in the aerospace sphere and the information-telecommunications space.*[59]

2.3 EW Procurement in Western MD

In general terms, the modernisation of Russia's conventional armed forces is proceeding faster and more intensively in the Western and Southern Military Districts. While this holds true in procuring modern EW assets, the presence of two EW brigades in Western MD, and only one in each of the others, favours this district in the acquisition process. This may also be influenced by the worsening of Russia-NATO relations.

The modernisation of Russia's conventional armed forces is proceeding faster and more intensively in the Western and Southern Military Districts

EW troops in Western MD have received ground, airborne and space-based modern EW equipment. In 2015 the *Leer*-3 UAV system was delivered and equipped with the *Sled*-KU integrated technical monitoring and communications intelligence collection station and LGSh-503 information leakage prevention equipment.[60] The *Leer*-3 aerodynamically "scatterable" (*zabrasyvayemyy*) jammer simultaneously blocks three mobile communications operators within a reported radius of up to 6 km and a control range of 60 km.[61] The *Beriev* A-50 *Mainstay* early warning and control aircraft, based on the Il-76MD, is equipped with the *Shmel* radio-technical complex and has entered service in Western MD. It weighs 190 tonnes, with a flight range of 7,500 km and a target acquisition range up

57. "The upgraded *Rychag*-AV system will be produced in 2016-17", KRET, last modified September 27, 2015, accessed July 10, 2017, http://oblik.msk.ru/en/news/4002/.
58. Sergey Denisentsev, "Okno vozmozhnostey dlya REB" [Window of opportunity for EW], *Voyenno-Promyshlennyy Kuryer*, 2 July 2014, http://www.vpk-news.ru/articles/20874 (accessed July 10, 2017).
59. Lastochkin and Falichev, "Kupol nad Minoborony", op. cit.
60. In June 2017, an EW training exercise was held in a Western MD Combined-Arms Army using the *Leer*-3 to suppress the navigation systems of a notional enemy's UAVs. See: "V obshchevoyskovoy armii ZVO provedena trenirovka grupp po bor'be s bespilotnikami" [In the combined-arms army of Western MD, training exercises were conducted for counter-UAV groups], Ministerstvo Oborony Rossiyskoy Federatsii, last modified June 29, 2017, accessed July 10, 2017 http://function.mil.ru/news_page/country/more.htm?id=12131418@egNews.
61. "Ucheniya voysk REB Zapadnogo voyennogo okruga" [Exercises of EW troops in Western military district], *Voyennoye Obozreniye,* July 22, 2016, https://topwar.ru/98370-ucheniya-voysk-reb-zapadnogo-voennogo-okruga.html (accessed July 10, 2017).

to 800 km, and the number of tracked targets is up to 300.[62]

The *Infauna* complex supports communications intelligence collection and communications jamming, and offers protection against short-range weapons and rocket launchers and against radio-controlled explosive devices; the system is being delivered to the VDV. Additional systems entering service in Western MD reveal the same pattern of rapid EW modernisation currently in progress. The district received the *Pelena*-1 high-powered ground jamming complex designed to jam early warning aircraft radars up to 250 km away. As noted, the *Borisoglebsk*-2 EW complex mounted on the MT-LBu entered service in 2015. This uses energy- and structurally-secure broadband signals to supply jam-resistant high-speed data transmission. The *Rtut*-BM system is similar and mounted on an MT-LB tracked chassis; reportedly a crew of two is capable of deploying the complex in ten minutes to protect personnel and equipment against munitions with radio proximity fuses in an area up to 50 hectares.[63] Western MD also received *Avtobaza* electronic counter countermeasures equipment, designed for passive detection of emitting radar systems and transmitting the coordinates, class and frequency band numbers of operating radars to an automated C2 facility.

EW jamming systems supplied to Western MD over the past three years included the *Zhitel* R-330Zh automated jammer, operating in the 100–2,000 MHz frequency band, with a range for communications intelligence collection and communications jamming of up to 15 km for ground targets and up to 200 km for airborne targets. During Exercise *Union Shield* 2015, a joint military exercise with Belarus, the *Zhitel* complex was used to jam a simulated enemy's UAVs.

Data collection and processing stations were procured in Western MD, such as the *Dzyudoist*, *Lorandit* and *Plavsk* complexes, as well as the *Svet*-VSG fixed radio monitoring equipment used for integrated technical monitoring.[64] The *Svet*-KU mobile EW complex became operational in 2012, and reportedly operates in the 30–18,000 MHz frequency band.[65]

Moreover, the *Krasukha*-4 mobile complex is an additional advanced technology asset in service with EW troops, distinguished by its multifunctionality and use of the latest software. *Krasukha*-4 allegedly counters on-board radars of the most advanced attack, reconnaissance and unmanned aviation at a range up to 300 km.[66] While the presence of these systems would not offer the Russian Armed Forces the opportunity to "switch off" NATO systems in any confrontation, it will mean that Alliance C4ISR will be targeted, and probably its operational tempo greatly reduced and some level of disruption caused. This EW capability is also an integral part of Russian A2/AD and would feature in response to any NATO effort to access and operate in the Baltic theatre.

EW capability is also an integral part of Russian A2/AD and would feature in response to any NATO effort to access and operate in the Baltic theatre

To examine the implication of EW modernisation further, it is useful to trace the recent evolution in EW combat support for Russian military operations. But the process of modernisation is ongoing, is likely to witness further significant progress in the 2020s, and will see continued state support in the GPV to 2025.

62. "Rossiya mozhet ispol'zovat' v Sirii samolet A-50" [Russia might use aircraft A-50 in Syria], *Rossiyskaya Gazeta*, January 14, 2016, https://rg.ru/2016/01/14/a50-site-anons.html (accessed July 10, 2017).
63. "Na vooruzheniye ZVO postupil kompleks REB Borisoglebsk-2" [EW complex *Borisoglebsk*-2 entered service in Western MD], *Zvezda,* April 1, 2017, https://tvzvezda.ru/news/opk/content/201704011213-cqzx.htm. (accessed July 10, 2017).
64. "Ucheniya voysk REB Zapadnogo voyennogo okruga", op. cit.
65. "V Zapadnyy voyennyy okrug prishla novaya tekhnika radioelektronnoy bor'by" [New electronic warfare equipment arrives at Western Military District], *Voyennoe.rf,* December 19, 2016, http://www. военное·рф/2016/3во62/ (accessed July 10, 2017).
66. "Kompleks 'Krasukha' polnost'yu oslepil istrebiteli na ucheniyakh ZVO" [Complex '*Krasukha*' has completely blinded fighter jets during the exercises of Western MD], *RIA Novosti*, August 14, 2015, https://ria.ru/defense_safety/20150814/1183503352.html (accessed July 10, 2017).

3. Advances in Russia's EW

3.1 From Chechnya to Ukraine: Russia's EW Support for Operations

Russia's advances in EW and in using the EMS as part of more integrated approaches to its combat operations can be seen in the evolution of these factors in the recent history of its military conflicts. Although these combat support elements were less well exploited during its early experiences in Chechnya, Russia's Armed Forces learned to make necessary corrections and tailored EW to suit a variety of operational requirements.[67] There is a clear learning curve in this regard between Chechnya I and II (1994–96, 1999–2009), while the brevity of the conflict with Georgia in August 2008 limited the role played by EW; this was not the case by the time of the intervention in Crimea and later in south-eastern Ukraine and in support of operations in Syria. Throughout this period, the General Staff studied the performance of EW assets, recommended adjustments, and incorporated lessons learned into procurement, organisational restructuring, training and the development of operational doctrine.[68] Consequently, Russia's Armed Forces have learned to harness EW tools as part of a strategic and tactical set of "force multipliers" that present severe difficulties for less technologically well-equipped and trained adversaries and potentially poses a challenge in the EMS for high-tech opponents.

Examining the course of this evolutionary process, with careful reference to Russia's experience of military conflicts and its exploitation of EW, reveals how these systems and specialists are used in conjunction with other combat elements. Essentially stunted during the 1990s, when it suffered from lack of investment, Russia's EW capability received a significant boost following the reform of the Armed Forces initiated in late 2008 with the restructuring of its EW forces and procurement of modern equipment. The conflicts in Ukraine and Syria provided opportunities to further test new EW systems in combat environments.[69] However, since more of these systems were deployed in the theatres of operation during the Ukraine conflict, our main focus will be on how this combat support feature was used to complement comparatively small forces, confirming that EW is now part of Russia's military preparations for conflict, an integral part of kinetic operations, and also used after kinetic contact.

Russia's Armed Forces have learned to harness EW tools that present severe difficulties for less technologically well-equipped adversaries and a challenge for high-tech opponents

3.1.1 Chechnya I and II, Georgia

In the course of the First Chechen War (1994–96), the Russian Armed Forces used the EW tools at their disposal to disrupt communications among Chechen fighters. The overall mission was controlled by a joint intelligence group, while EW assets were diffused among the Ground Forces' Corps and 4th Air Army. However, although there was EW use in Russian operations, these were hampered by a lack of trained personnel, undermanning in specialist units and personnel having to be deployed from across the Russian Federation to compensate. In 1994, EW forces acted behind frontline Russian troops in key operations including the storming of Grozny, tasked with tactical suppression of enemy forces' communications. A number of weaknesses in the Russian Ground Forces' use of EW during Chechnya I were identified to include: shortage of trained specialists and

67. I.A. Ivanov, I. Chadov, "Soderzhanie i rol' radioelektronnoy bor'by v operatsiyakh XXI veka" [The contents and role of electronic warfare in the operations of the 21st century], *Zarubezhnoye Voyennoye Obozreniye* No. 1 (2011): 14–20, accessed July 10, 2017, http://pentagonus.ru/publ/soderzhanie_i_rol_radioehlektronnoj_borby_v_operacijakh_xxi_veka/80-1-0-1700.
68. M. Boltunov, *Zolotoye ukho voyennoy razvedki* [A golden ear of military intelligence] (Moscow: Veche, 2011): 66–71, 88–102, 114–7.
69. Author interviews with NATO EW specialists, Brussels, June 2017.

consequent undermanning of EW units; limited tactical readiness; unreliability of jamming stations; and complications with using EW equipment on the march. By August 1996, for example, Russian units were unable to jam enemy communications during the militants' assault on Grozny.[70]

In the hiatus between the two conflicts, the Russian General Staff sought to remedy many of these failings. Despite the challenges of operating in very mountainous terrain, during Chechnya II Russia's use of EW became better organised and able to achieve greater success in disrupting enemy communications, based on the introduction of new equipment and forming an EW command centre in the 58th Army, capitalising on an automated command post using RP-330KP, aiding C2 of subordinate units. EW forces also helped to facilitate operations involving Russian Ground Forces units and those drawn from other power ministries. EW forces also made improved use of jamming and direction-finding equipment, and set up constant monitoring of enemy communications on the territory. It was also used to disrupt militant radio-controlled explosive devices. Nevertheless, despite undoubted advances in the use of EW, improved organisation and local coordination, the experience gained was quite limited in terms of what the Chechen fighters could deploy. During these conflicts, Russian military EW was up against mainly commercial communications rather than military-grade systems. Moreover, its EW assets did not have to contend with either advanced weapons systems or sophisticated air defence assets.[71]

The conflicts in Ukraine and Syria provided opportunities to further test new EW systems in combat environments

While Russia's use of EW during Chechnya I and II witnessed improvements and evolution, the experience gained during counterinsurgency operations had to be built upon to develop a wider capability that might be applied in other operational environments, and especially in combined-arms operations. The Five-Day War with Georgia in August 2008 afforded a brief opportunity to field-test some fresh advances. Small numbers of EW personnel were embedded into battalion tactical groups deployed in South Ossetia. The Russian Air Force was later heavily criticised for its overall performance in the conflict and its rather belated entry to suppress Georgia's air defences. Indeed, only following the loss of five aircraft did Russia's military deploy air assets including helicopters to conduct EW to counter civilian and military radars. An-12PP aircraft conducted daily patrols to support operations in South Ossetia and Abkhazia, while Mi-8PPA and Mi-8PSM-PG helicopters operated closer to front lines to provide additional anti-radar capability. Furthermore, ECM may have been used to jam Georgia's Unmanned Aerial Systems (UAS).[72]

Despite the challenges of operating in very mountainous terrain, during Chechnya II Russia's use of EW became better organised and able to achieve greater success

Georgia's mountainous terrain also greatly limited the coverage of Russian fixed-wing aircraft- and helicopter-mounted jammers.[73]

70. Vladimir Gordiyenko, "Stoletiye radioelektronnoy bor'by" [Centenary of electronic warfare], *Nezavisimoye Voyennoye Obozreniye*, April 11, 2003, http://nvo.ng.ru/history/2003-04-11/5_reb.html (accessed July 10, 2017).
71. A.I. Paliy, *Radioelektronnaya bor'ba v voynakh i vooruzhennykh konfliktakh* [Electronic warfare in wars and armed conflicts] (Moscow: VAGSH, 2007): 64–72.
72. Anton Valagin, "Chto napugalo amerikanskii esminets" [What scared the American destroyer], *Rossiyskaya Gazeta*, April 30, 2014, www.rg.ru/2014/04/30/reb-site.html (accessed July 10, 2017).
73. Andrey Mikhaylov, "Pyatidnevnaya voyna: itog v vozdukhe" [Five-day war: outcome in the air], *Vozdushno-Kosmicheskaya Oborona*, January 30, 2009, http://www.vko.ru/voyny-i-konflikty/pyatidnevnaya-voyna-itog-v-vozduhe (accessed July 10, 2017).

But, despite the haphazard use of EW in support of combat operations and to aid force protection, one success lay in the pre-production deployment of the Su-34 with its onboard *Khibiny* self-defence system. In this context, while its use was fleeting, the Su-34 and its EW capability proved effective assets against air defence systems. However, given the reorganisation of Russia's EW forces and the steady increase in modernising its equipment inventory attended by doctrinal and operational shifts taking place in the military, and occurring on the back of the Georgia conflict, by 2014–15 Moscow's operations in Ukraine and Syria marked more clear advances in EW capacity.[74]

3.1.2 Syria: Force Protection

Russia's military operations in Syria, commencing in late September 2015 and largely restricted to air strikes, though also involving limited on-the-ground support both for Special Forces and military advisers in the training of the Syrian Arab Army (SAA), required EW support.[75] Initially, this seems calibrated to limited force protection in terms of air assets and base protection, but following the shooting-down by the Turkish Air Force of a Russian Su-24M in late November 2015, air defence and EW components were stepped up. In the months following the incident, Moscow sought to strengthen air defence and EW support in key locations in Syria to enhance A2/AD.[76] This seems to have been limited in scope, intended to boost the impression that the Russian forces in theatre were well supported and adequately protected, but other than possible repeat attacks by the Turkish Air Force, the "threat" as such was neither especially high-tech nor plausible.[77]

Western commentaries frequently characterised key dynamics of Russian military operations in Syria as involving "experiments" designed to test newly introduced assets or field-test prototype weapons systems or platforms. There certainly was a degree of experimentation, particularly in field-testing network-centric systems and tactics or simply using combat operations as an invaluable opportunity to train VKS personnel, but there is no substantive evidence to support the assertion that Russian forces were rehearsing for combat against NATO. The apparent afterthought to boost air defences in Syria two months after initial deployment suggests that the Kremlin did not take seriously the escalation of conflict in the theatre of operations.[78] Furthermore, unlike in Crimea and the Donbas, EW testing appears to have been narrower and modest in scope. As far as is possible to ascertain, the Russian EW systems deployed in Syria were focused on base and force protection, rather than serving as a chance to show off systems in a wider effort to send "strategic messages".[79]

In October 2015, Russia deployed the *Krasukha*-4 ground-based EW system to its Khmeimim airbase in Latakia. The *Krasukha*-4 is a multifunctional jammer, with conflicting reports about its capabilities; it appears mainly designed to jam airborne radars.[80] Deploying the system to Khmeimim was probably part of a process to support other air-defence assets to protect the base from air attack. In terms of testing, it is likely that the Russian military wanted to field-test the system to check its reliability, since there had been reports raising doubts about the *Krasukha*-4 in the

74. Mikhaylov, "Pyatidnevnaya voyna".
75. EW receives surprisingly little coverage in M.Y. Shepovalenko (ed.), *Siriyskiy Rubezh* [Syrian Frontier] (Moscow: CAST, 2016): 105–20. Most coverage in Russian sources tends to talk up or exaggerate the EW contribution to A2/AD in Syria.
76. "Turetskiy Korall protiv rossiyskogo Triumfa: sistemy REB u granits Sirii" [Turkish *Korall* against the Russian *Triumf*: EW systems on the borders of Syria], *Voyennoye Obozreniye,* December 3, 2015, http://topwar.ru/87224-tureckiy-korall-protiv-rossiyskogo-triumfa-sistemy-reb-u-granic-sirii.html (accessed July 10, 2017).
77. "V Sirii poyavilos' rossiyskoye radioelektronnoye oruzhiye—Times" [Russia's electronic weapons appeared in Syria—Times], *KorrespondenT.net*, October 7, 2015, http://korrespondent.net/world/3573109-v-syryy-poiavylos-rossyiskoe-radyoelektronnoe-oruzhye-Times (accessed July 10, 2017).
78. Aleksandr Tikhonov, "V tsentre vnimaniya oboronka" [Defence industry in focus], *Krasnaya Zvezda*, May 12, 2016, http://redstar.ru/index.php/component/k2/item/28841-v-tsentre-vnimaniya-oboronka (accessed July 10, 2017); Yuriy Borisov and Oleg Falichev, "Tyazhelaya raketa nelegkoy sud'by" [Heavy rocket of a difficult fate], *Voyenno-Promyshlennyy Kuryer*, May 11, 2016, http://vpk-news.ru/articles/30571 (accessed July 10, 2017).
79. Borisov and Falichev, "Tyazhelaya raketa".
80. "Razvedyvatel'nyye samolety, sistemy radioelektronnoy bor'by i vysokotekhnologichnaya voyna Rossii v Sirii" [Reconnaissance aircraft, electronic warfare systems and Russia's high-tech war in Syria], *Russia Insider*, October 31, 2015, http://russia-insider.com/ru/oborona-i-bezopasnost/razvedyvatelnye-samolety-sistemy-radioelektronnoy-borby-i (accessed July 10, 2017).

past.[81] Some additional clues about its role in Syria are alluded to in some public reporting on the various deconfliction agreements Moscow worked out with other parties in the autumn of 2015. Moscow requested that the details of its deconfliction agreement with Washington should not be released. However, its agreement with Israel reportedly included some reference to "electromagnetic arenas", suggesting that concern about VKS activity in Syria extended to the use of EW.[82]

In addition to the *Krasukha*-4, the most readily identifiable EW systems in Syria were the *Khibiny* and *Leer*-3; though some other assets may have been moved in and out in support of operations or to experiment with the A2/AD mix, these were consistently present and certainly being used long-term during the Syria campaign. Setting aside mythical claims concerning the *Khibiny*, at a more serious level there is much confusion in Russian sources about the entire *Khibiny* series and their subsystems. *Khibiny* ECM pods were frequently in evidence on the wingtips of Su-30SM, Su-34 and Su-35S platforms deployed in Latakia; these act as aircraft self-protection and as jammers.[83] The General Staff would have paid close attention to how these pods functioned in combat conditions, in addition to referencing meteorological conditions. It is also possible these were used to detect coalition radar emissions.

Russian EW systems deployed in Syria were focused on base and force protection, rather than serving as a chance to show off systems in a wider effort to send "strategic messages"

However, it is surprising that with all the combat-testing of systems occurring in the Syria operations, there was no public sighting of the larger pods under the fuselage or wings necessary for the air group protection capability. The smaller *Khibiny* pods on the wingtips were only about individual aircraft protection and jamming. In this sense, the deployment of the Su-34 is of special interest since it will, in the future, receive the larger *Tarantul* ECM pod currently undergoing state trials; this is likely to be in support of the *Khibiny* system, but there is no evidence that the trials ever shifted to testing the prototype *Tarantul* in Syria.[84] Indeed, the absence of the larger ECM pods for air group cover may explain why most airstrikes were conducted by the older Su-24 and Su-25s, operating without escorts.

Efforts to support more sensitive ground operations alongside the SAA against enemy forces certainly relied heavily upon the *Leer*-3 system. It is highly likely that this asset aided SAA assaults on opposition forces since it is used to jam mobile phone networks and would have degraded the ability of these forces to communicate with each other.[85] It is also user-friendly in such an operational environment since it involves the *Orlan*-10 UAV, removing the jammer/operator from harm's way. It seems that the system is capable of not only jamming GSM networks but also sending false

81. "Krasukha-4 v Sirii: god elektronnogo shchita na Khmeymim" [*Krasukha-4* in Syria: a year of electronic shield over Khmeimim], *Defence.ru*, October 11, 2016, https://defence.ru/article/krasukha-4-v-sirii-god-elektronnogo-schita-nad-khmeimim/ (accessed July 10, 2017); "V Siriyu pribyli noveyshyye rossiyskiye kompleksy radioelektronnoy bor'by 'Krasukha-4'" [The newest Russian electronic warfare complexes *Krasukha-4* arrived at Syria], *Voyennyy Informator*, October 5, 2015, http://military-informant.com/airforca/v-siriyu-pribyili-noveyshie-rossiyskie-kompleksyi-radioelektronnoy-borbyi-krasuha-4.html (accessed July 10, 2017).
82. Barbara Opall-Rome, "Russia, Israel to broaden coordination in Syria", *OSnet Daily*, December 1, 2015, http://osnetdaily.com/2015/12/russia-israel-to-broaden-coordination-in-syria/ (accessed July 10, 2017); Neil MacFarquhar, "U.S. agrees with Russia on rules in Syrian sky", *New York Times,* October 20, 2015, www.nytimes.com/2015/10/21/world/middleeast/us-and-russia-agree-to-regulate-all-flights-over-syria.html?_r=0 (accessed July 10, 2017).
83. Yevgeniy Saltykov, "Bitva za efir: rossiyskiye sistemy REB pokazali v Sirii svoyu effektivnost'" [Battle for airwaves: Russian EW systems showed their effectiveness in Syria], *Vesti*, March 18, 2016, http://www.vesti.ru/doc.html?id=2732816 (accessed July 10, 2017).
84. *Tarantul* is an EW suite in development for the Su-34 fighter bomber to conceal aircraft or a group of strike aircraft from enemy radar. The *Tarantul* ECM system is being developed as part of the modernisation programme for the Su-34 in the 2020s.
85. Alex Alexeyev, "Voyna v efire. Chast' 1" [War on airwaves. Part 1], *Voyennoye Obozreniye*, May 22, 2017, https://topwar.ru/116054-voyna-v-efire-chast-1.html (accessed July 10, 2017).

text messages to mobile phones. Less certain are the claims it can be used over wider areas to gain remote access to mobile phones in order to send false reports or issue calls to surrender. Equally, some Russian sources suggesting that when the *Leer*-3 was first deployed to Syria it could only function against 3G and 4G networks, though this remains unconfirmed.[86]

A number of observations can be made about Russia's deployment of EW assets to support its operations in Syria. First, the key role assigned to EW was force protection, aiding air defence and facilitating on-the-ground operations conducted by Special Forces and the SAA. Second, many of these systems were deployed in this context to test and further refine EW capabilities. Equally, a degree of testing network-centric operations occurred, with support from EW, while additional testing related to how to construct sufficient A2/AD in the vicinity of Russian concentrations of military assets in Tartus and Latakia and at temporary forward operating bases.[87] In the context of force protection, EW systems doubtless played a significant role in reducing loss of aircraft in combat, as well as protecting smaller numbers of ground forces deployed in support of the SAA. It is likely that some of the EW activity may be directed at collecting EM signature information on NATO aircraft to build their EM database.

3.1.3 Crimea to the Donbas: Invisible Support

In stark contrast to Russia's operations in Syria, the seizure of Crimea and the war in the Donbas relied more heavily on extensive EW use, and the conflict in south-eastern Ukraine has served as a test bed for Russian experimentation in EW systems. The performance of the Ukrainian Armed Forces in the loss of Crimea has been assessed and outlined in sufficient detail elsewhere.[88] It is important to note that EW loomed large in Russia's intervention in the Donbas, facilitating smaller numbers of military personnel in their task of presenting a formidable challenge to the Ukrainian Armed Forces.[89] However, Russia's use of ECM both in the operation to seize Crimea (involving no combat) and later throughout the conflict in south-eastern Ukraine continues to be misunderstood as an important factor in the success of both by aiding proxy forces and destabilising sizeable areas of Ukraine using relatively small forces.

The seizure of Crimea and the war in the Donbas relied heavily on extensive EW use, and served as a test bed for experimentation

As Michael Kofman *et al* explain, the Western preoccupation with reading into Russian operations in the Donbas as an overall "hybrid war" was, at the very least, myopic:

> *Some Western analysts characterized the campaign in Eastern Ukraine as a hybrid war; this perspective is incorrect. Rather, the conflict from February to August cycled through four different types of warfare: political, irregular, hybrid, and conventional. There are no indicators that Russia intended to conduct a hybrid war, despite arguments in some circles that such a doctrine and approach exists within the thinking of the General Staff of the Armed Forces of the Russian Federation. Little about the early days of the conflict in Ukraine is indicative of the supervision and involvement of the General Staff. Russia's selection of tactics was not doctrinally driven but, rather, it was a series of improvised responses to Ukrainian resistance.*[90]

Indeed, Western policymakers were also quick to praise the "restraint" shown by Kyiv in resorting to military force as events unfolded

86. Author interviews with Israeli defence specialists, Washington DC, June 2017.
87. O.V. Tikhanychev, "O roli sistematicheskogo ognevogo vozdei'stviya v sovremennykh operatsiyakh" [On the role of a systematic fire support impact in contemporary operations], *Voennaya Mysl'* No. 11 (2016): 16–20.
88. See Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND, 2017): 22–5, 67–70.
89. Author interviews with Ukrainian EW experts, Kyiv, May 2017.
90. Kofman et al, *Lessons from Russia's Operations*: 69.

EW System	Function
RB-341V Leer-3	GSM communications jamming
RB-301B Borisoglebsk-2	Automated jamming system (detection, direction finding, analysis and suppression of HF/VHF radio communications). Includes R-330KMV command post and several jamming stations
R-934UM	Radio jamming station (detection, direction-finding, analysis and suppression of VHF/UHF radio communications). Part of R-330M1P Diabazol automated jamming system
R-330Zh Zhitel	SATCOM/GPS/GSM jamming station (detection, direction-finding, analysis and suppression of UHF radio signals). Part of R-330M1P Diabazol automated jamming system
Shipovnik-Aero	UAV Interception System
Torn	Radio jamming station (unknown specifications; currently not in service)
Rtut-BM	Radio proximity fuse jamming station (protecting personnel and equipment from munitions using proximity fuses)
RB-636AM2 Svet-KU	Monitors airwaves and tracks various radio emitting sources
R-318T Taran	COMINT system. Includes command post and several stations operating in HF/VHF/UHF range
MKTK-1A Djudist	Radio control and information protection system (detection, direction finding and analysis of radio signals). Intended to assist with emission control

Figure 6: Russian EW systems deployed in the Donbas

in Crimea, a point frequently shared by NATO analysts in private conversations with the author.[91] Nonetheless, careful reference to the details surrounding Russia's insertion of troops in Crimea including Special Operations Forces and supporting units actually exposes how pivotal was the role of Russian EW.

As various highly trained Russian specialist military personnel fanned out across the peninsula surrounding Ukrainian military bases, ECM was exploited to cut off Ukrainian forces from communicating with mainland Ukraine. Severing C2 of these Ukrainian military facilities took advantage of local military personnel depending upon stationary and wired means of communication, allowing Russian *Spetsnaz* units to quickly cut these links and isolate the Ukrainian military facilities in Crimea. By 11 March 2014, for example, as more ground forces were moved across the Kerch Straits into Crimea, *Leer*-2, *Lorandit* and *Infauna* EW systems were in evidence.[92]

By contrast, in the case of the Donbas, a large number of Russian EW systems appeared and was moved across the porous border with Ukraine (see Figure 6), providing opportunity to experiment with these EW systems. For example, on 13 May 2017, the OSCE Special Monitoring Mission (SMM) observed a Russian-made *Orlan*-10 UAV flying across the road from Makiivka (12 km north-east of Donetsk) towards Donetsk City. The frequently sighted *Orlan*-10 functions as part of the *Leer*-3 EW system.[93] However, as far as possible, a number of systems have been identified that played a more enduring role in Russia's EW support for operations and for separatists. These seem to be part of a wider effort to use the Donbas as a fundamental testing ground for Russia's Armed Forces.

As already noted, EW assets and specialist personnel operate within Russia's Ground Forces in the manoeuvre units. Part of the challenge in the Donbas was to provide this support, frequently indirectly through the

91. Author research interviews in Mons, December 2015 and Rome, September 2014.
92. Kolesova and Nasenkova, *Radioelektronnaya bor'ba*, op. cit.: 229.
93. "Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 14 May 2017", OSCE Special Monitoring Mission to Ukraine, last modified May 15, 2017, accessed July 10, 2017 http://www.osce.org/special-monitoring-mission-to-ukraine/317386. *Orlan*-10 UAVs have also been shot down by the Ukrainian Armed Forces during the conflict in the Donbas.

training and use of local proxies, though some Russian EW specialists may well have been embedded with separatist units. This has allowed the Russian military to gain vitally important experience in exploiting EW assets in a range of different types of operation and to tailor this to suit the needs of a unique operational environment. Only in the more direct intervention requiring Russian troops to lead in combined-arms operations to rout enemy forces in Ilovaysk and Debaltseve is insight offered into how this might be integrated into future regular operations by Russia's Armed Forces.[94] In the context of "plausible deniability", much of the Russian EW activity in the Donbas was necessarily clandestine and difficult to assess.[95]

EW was used in the Donbas conflict by all parties. On the separatist side, this covered the broad range of EW operations, from blocking mobile phone signals to targeted jamming of military communications systems and radars. The OSCE SMM was frequently impeded in its work due to the use of ECM to target OSCE *Schiebel* S-100 Camcopter UAVs; these would either crash or enter auto-return mode. EW usage in the conflict can be categorised as follows:

- EW to target Ukrainian UAS by jamming controller or GPS signals;
- ECM to disrupt electronically fused munitions ranging from artillery to mortars;
- Disruption of enemy communications: in some parts of the region, no communications systems function;
- Targeting C2: Russian EW assets detect electromagnetic emissions, which can be located and targeted.[96]

During the conflict, due to the active use of EW by Russian and proxy forces, the Ukrainian Armed Forces learned to operate in a hostile EW environment. This included limited training and input from Western militaries and the provision by the US of small numbers of Single Channel Ground and Airborne Radio System (SINGGARS), but radio net encryption is not widespread in Ukraine's military operations. Russia certainly deployed into the Donbas both in-service EW systems and new equipment undergoing trials.[97] Moreover, in terms of "sightings" of Russian EW equipment, RB-341V *Leer*-3 EW vehicles and *Borisoglebsk*-2 loomed large. Yet, according to eyewitnesses, these tended to be placed well away from the front lines and closer to the Russian border.[98]

Although details are sketchy because Ukraine's General Staff has designated the area of EW as secret, open-source reporting and author research interviews were able to identify the most likely innovative features of Russia's EW operations in the Donbas. First, the use of highly mobile tactical EW groups throughout the conflict, constantly changing location to avoid destruction under fire; though elements of this approach were visible in earlier local conflicts, it appears that the Russian General Staff devised methods of deploying independent tactical EW groups able to operate on the move. Second, Russian EW units also experimented with new EW algorithms. The main innovation, however, lay in the much larger-scale use of EW in support of operations. It also appears that Russia's General Staff assigned much importance to the testing of new tactics and the effectiveness of automated and mobile systems; there are indications that on this basis—and not operations in Syria—the General Staff introduced a new EW manual into the Russian Armed Forces in early 2017.[99]

94. Paul Robinson, "Explaining the Ukrainian Army's Defeat in Donbass in 2014", in J.L. Black and Michael Johns (eds), *The Return of the Cold War: Ukraine, the West and Russia* (London: Routledge, 2016); Roger N. McDermott, *Brothers Disunited: Russia's Use of Military Power in Ukraine* (Fort Leavenworth: Foreign Military Studies Office, 2015), https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/197162 (accessed July 10, 2017). Charles K. Bartles and Roger N. McDermott, "Russia's Military Operation in Crimea: Road-Testing Rapid Reaction Capabilities", *Problems of Post-Communism* Vol. 61, No. 6 (2014): 46–63.
95. Bartles and McDermott, "Russia's Military Operation in Crimea".
96. Author interviews with members of the OSCE SMM, Kyiv, May 2017; interviews with NATO EW specialists, Washington DC, June 2017.
97. Author interviews with members of the OSCE SMM, Kyiv, May 2017; interviews with NATO EW specialists, Washington DC, June 2017.
98. Author interviews with members of the OSCE SMM, Kyiv, May 2017.
99. Author interviews with Ukrainian EW specialists, Kyiv, May 2017; "'Dobyto v shakhte': Na vooruzhenii terroristov LNR stoit rossiyskaya perenosnaya stantsiya razvedki 'Kredo-M1'. Foto" ["Mined from a mine": weaponry of LNR terrorists includes a Russian mobile reconnaissance station *Kredo-M1*. A photo], *Begemot*, March 26, 2017, http://begemot.media/news/dobyto-v-shahte-na-vooruzhenii-terroristov-lnr-stoit-rossijskaya-perenosnaya-stantsiya-razvedki-kredo-m1-foto/ (accessed July 10, 2017).

3.1.4 EW in Action: Ilovaysk and Debaltseve

On two occasions during the Ukraine conflict, Russian units and equipment intervened directly to shore up the separatists: in August 2014 in Ilovaysk and in January–February 2015 at Debaltseve during the talks resulting in Minsk II. These were marked by typical combined-arms approaches to warfare and in each case Russian and proxy forces quickly secured local victory. However, also present in each instance were EW assets and the use of EW in preparing, conducting and completing the local operation.[100]

In Ukraine, the Russian General Staff devised methods of deploying independent tactical EW groups able to operate on the move

In the case of the strategically important Ilovaysk, located 25 km east of Donetsk, a series of kinetic contacts precipitated the encirclement of Ukrainian forces by Russia's Armed Forces units from Pskov and Kursk; this involved the deployment of battalion tactical groups, reconnaissance and sabotage groups including EW units, transferred from Russian territory to the conflict zone.[101] Ahead of the engagement, EW assets were also arriving in the area in preparation for the ensuing operation; these were to be used to suppress enemy communications.

These systems included: *Leer*-2 complexes; 1L262E *Rtut*-BM; stations to jam GPS signals and UAV data links such as the *Shipovnik-Aero*, or *Krasukha*-2 and *Krasukha*-4 for suppression of enemy Intelligence, Surveillance and Reconnaissance (ISR); and the automated jamming complex *Borisoglebsk*-2. Russian EW assets were tasked with the following: suppressing radio communications at tactical and operational levels, fixing and locating enemy forces by identifying EMS usage, disrupting C2, blocking mobile phone networks and spreading false information as part of PSYOPS.[102]

In order to achieve these goals, EW was deployed and used at concentric distances from the area of operations. Closest to the kinetic action, at distances of 1 to 3 km, RB-531B *Infauna* disrupted Ukrainian military communications, supported by *Rtut*-BM, *Leer*-2 and *Lorandit* complexes; these were intercepting and direction-finding against GSM use. In the range of 15–30 km outside the line of contact, Russian EW systems included Leer-3, R-330ZH *Zhitel*, R-934UM and the automated *Borisoglebsk*-2. Further still from the line of contact, at 60–240 km air suppression systems were in use, such as *Shipovnik*-Aero, *Krasukha*-2 and the DRLOU A-50 airborne early warning aircraft. In other words, at these distances some of the EW operations were being conducted from Russian territory.[103]

Two particularly important areas of Russian EW use in Ilovaysk should be highlighted: fixing and targeting for artillery fire and complementary exploitation of EW to facilitate PSYOPS. Russian EW systems would detect enemy communications transmissions, including mobile phones, to provide target information to conduct artillery strikes. Moreover, by disrupting enemy's mobile networks and transmitting data, some instances involved Ukrainian personnel receiving negative text messages on their phones, aimed at undermining morale.[104] Such PSYOPS and EW integration may not have been on a wide scale, but it certainly took place sporadically and

100. Author interviews with members of the OSCE SMM, Kyiv, May 2017.
101. Author interviews with Ukrainian EW specialists, Washington DC, June 2017.
102. Vyacheslav Gusarov, "Osobennosti organizatsii i vedeniya radioelektronnoy bor'by v boyakh za Ilovaysk. Analitika IS" [Peculiarities of battle order and conduct of electronic warfare in the battles for Ilovaysk. Analysis of IS], *Informatsionnoye Soprotivleniye,* December 5, 2016, http://sprotyv.info/ru/news/kiev/osobennosti-organizacii-i-vedeniya-radioelektronnoy-borby-v-boyah-za-ilovaysk-analitika (accessed July 10, 2017).
103. Gusarov, "Osobennosti organizatsii i vedeniya radioelektronnoy bor'by".
104. Author interviews with Ukrainian EW specialists, Kyiv, May 2017. It is unlikely that this could have been carried out on a wide scale, but rather it used deployed EW assets to target pockets of resistance. Equally, targeting enemy mobile phones in this way may also imply Russian access to sensitive Ukrainian military personnel details.

among significant numbers of Anti-Terrorist Operation (ATO) personnel.[105]

In January–February the area around Debaltseve witnessed a surge in fighting, with Russian-led operations focusing on securing the strategically important transport hub in Luhansk region. Russian and separatist forces saw the need to "tidy up" the area by taking Debaltseve despite the diplomacy surrounding Minsk II. As in Ilovaysk, Russian EW systems were deployed in advance to prepare the battlefield and during the combat operations. What differed on this occasion was the use a comprehensive technical EW monitoring group tasked with monitoring the EMS, apparently using the experience gained earlier in Ilovaysk. EW assets were deployed by Russia's Armed Forces for direction-finding/geolocation, disrupting enemy communications among other features. This also used automated jammers. The overall scheme of the EW operations implemented an automated cycle of radio-survey/detection, jamming and intelligence analysis, working closely with SIGINT and providing information in real time. Russian groups again used EW systems, most likely *Leer*-3, to facilitate PSYOPS to target ATO personnel; with numerous reports of Ukrainian military servicemen receiving text messages aimed at undermining their morale. Likewise, the high level of accuracy in artillery fire stemmed from successful employment of EW to fix and locate enemy targets by identifying mobile phone emissions in communications between ATO servicemen.[106]

PSYOPS and EW integration may not have been on a wide scale, but it certainly took place among significant numbers of Anti-Terrorist Operation personnel

The importance of Russian EW in these kinetic operations in Ukraine offers deeper insight into how such assets will be exploited in future conflict. At a military theoretical level, as Korolyov, Kozlitin and Nikitin argued in their article in *Voyennaya Mysl'*, the development of Russia's EW capability is evolving exponentially towards placing this at the very forefront of its future operations, and this eventually might merit its designation as an arm of service, rather than playing a purely combat support role:

> *This is due to the fact that, being an arm of the service, the EW forces and weapons do not support combat actions, but directly participate in them, when realizing operational missions to disorganize the adversary's command and control over his troops and weapons. At that, their target orientation in combat use lies in disorganizing the adversary's hands-on command and control over combat actions. Moreover, evaluating its efficiency can be carried out not only according to the classic scheme for disrupting current and organizational commanding influences by delaying timely information support to the DMs (decision makers), but*

The development of Russia's EW capability is evolving exponentially towards placing this at the very forefront of its future operations

105. See "Electronic warfare by drone and SMS: How Russia-backed separatists use 'pinpoint propaganda' in the Donbas", *Atlantic Council's Digital Forensic Research Lab*, May 18, 2017, https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696 (accessed July 10, 2017).

106. Vyacheslav Gusarov, "Taktika rossiyskikh grupp REB v boyakh za Debal'tsevo. Analitika IS" [Tactics of the Russian EW groups in the battles for Debaltsevo. Analysis of IS], *Informatsionnoye Soprotivleniye,* January 5, 2017, http://sprotyv.info/ru/news/kiev/taktika-rossiyskih-grupp-reb-v-boyah-za-debalcevo-analitika (accessed July 10, 2017); see also "Radioelektronnaya bor'ba rossiyskikh terroristicheskikh sil v nachal'noy faze voyennogo konflikta v Ukraine" [Electronic warfare by the Russian terrorist forces during the initial phase of the armed conflict in Ukraine], *Informatsionnoye Soprotivleniye*, September 20, 2016, http://sprotyv.info/ru/news/kiev/radioelektronnaya-borba-rossiyskih-terroristicheskih-sil-v-nachalnoy-faze-voennogo (accessed July 10, 2017).

also by misguiding them with skilfully warped (false) information, opportunely relayed to specific governing bodies through the Common Information and Telecommunications Environment.[107]

Russia's military actions in the Donbas, more than any previous conflict, not only afforded valuable opportunities for experiment but also marked a closing of the gap between the theory underlying EW and its application in support of combat operations. Many of these features were present, ranging from warping information in support of PSYOPS, to jamming, blocking and disrupting the adversary's communications and radars and disorganising the enemy's ability to conduct C2 during operations.[108]

While this may be a long way from achieving the status of an arm of service, it is certainly already providing key combat support in Russian military operations. Ukraine's Armed Forces were singularly unprepared for Russian use of EW in support of its intervention in Crimea and south-eastern Ukraine, though they learned to operate in a hostile EW environment and made some progress as the conflict evolved. Nevertheless, to avoid hyperbole regarding Russia's Armed Forces and its growing EW capability it should be stated that these events occurred in the context of facing a technologically inferior adversary.[109] And so the question arises as to what Russia's advances in developing better EW capabilities means for NATO and the security of its members on its Eastern Flank.

If conflict with Russia ever erupts on NATO's Eastern Flank, the first sign of activity will be in the EMS—and in this spectrum the initiative and advantage will be determined

Conclusions: Implications for NATO

Russia has made considerable headway in its efforts to adopt innovative approaches to warfare, including its experiments with network-centric capability, exploring ways of using and gaining advantage over an adversary in an information environment. This relates primarily, though not exclusively, to enhancing the speed of decision-making through the integration of automated C4ISR: a process also in play in the EW forces. Russian military planners have thus narrowed the gap between military science and actual change to military capability.[110] EW is playing an increasingly integral role in the pursuit of "force multipliers", as is evidenced in Russia's more recent combat experience.[111] However, the exploitation of EW assets in support of operations in south-eastern Ukraine offers very limited lessons for NATO as such, since the Alliance can field advanced technological assets way beyond anything that Kyiv can bring to bear. Moreover, some Russian claims to be able to completely technologically degrade the EMS are palpably false.

Nevertheless, there are important implications for the Alliance in the progress made in EW by Russia's Armed Forces, as well as the likely long-term persistence of these trends in military modernisation and transformation. Above all else, it requires recognition that, through such "force multipliers", the end result of the ongoing transformation of Russian's Armed Forces will offer a conventional capability way beyond that possessed by the Soviet legacy force of the 1990s.[112] If conflict with Russia ever erupts on NATO's Eastern Flank, the first sign of activity will be in the EMS—and in this spectrum the initiative and advantage will be determined. Moscow appears to perceive this as an area of possible weakness on the part of the Alliance, and has

107. Korolyov, Kozlitin and Nikitin, "Problemy opredeleniya sposobov boevogo primeneniya", op. cit.
108. Author interviews with Ukrainian EW specialists, Washington DC, June 2017.
109. Author interviews with NATO EW specialists, Washington DC, June 2017.
110. Lastochkin and Falichev, "Kupol nad Minoborony", op. cit.; Korolyov Kozlitin and Nikitin, "Problemy opredeleniya sposobov boevogo primeneniya", op. cit.
111. Gusarov, "Taktika rossiyskikh grupp REB", op. cit.
112. Ivanov, "Soderzhanie i rol' radioelektronoy bor'by", op. cit.

therefore invested in further strengthening this capability. This means that NATO must change its approaches to policy, doctrine, organisation, capabilities, training, tactics and procedures, and exercise scenarios.[113]

These advances have not gone unnoticed by some US EW officers. In December 2015, Colonel Jeffrey Church, chief of the Army staff at the Pentagon's Electronic Warfare Division, identified the extent to which the Russian military may have organisationally surpassed their American counterparts in terms of EW. Addressing a meeting of EW specialists in Washington DC, Church explained:

> *The Russians train to it. They have electronic warfare units, they have electronic warfare equipment that those trained soldiers use, and then they incorporate it into their training. We do not have EW units, we have very little equipment, and we do very little EW training. It's not that we could not be as good as or better than them, it's just that right now we choose not to.*[114]

The Alliance has much to do to rectify the neglect of the emergence of Russia as a competitor in the EMS

And such arguments certainly contributed to the effort to draft and implement a new US EW Strategy in early 2017; however, the Alliance has much to do to rectify the neglect of the emergence of Russia as a competitor in the EMS. However, in terms of boosting reassurance and deterrence efforts in the Baltic region, NATO has a long way to go, bearing in mind the aforementioned considerable Russian EW capability, since this capability feeds into Russian A2/AD approach.

A potentially important partner for the Alliance in boosting security in the Baltic states is Israel. Cooperation on EW has long existed between Israel and the United States, and this can be extended to other members of the Alliance. Since the Baltic states are already "tech-savvy", there is an existing foundation to strengthen effective EW and cyber-warfare capability; Israeli specialists can assist in developing SIGINT capabilities in the Baltic region to help address potential emission control and limit the effectiveness of Russian eavesdropping. Israeli EW specialists could also offer valuable assistance to develop concepts that will maximise the effectiveness and coordination of various EW elements, including their coordination with one another and with cyber- and kinetic attacks, based on the Israeli Defence Forces' extensive experience under real combat conditions.[115]

Likewise, Israeli EW specialists can assist in developing the Alliance's UAV-borne EW capability, since electronic protection and attack capabilities for UAS will grow in importance as more capable and more expensive UAS are fielded, particularly those expected to operate in EMS-contested environments. Israel offers both EP and EA solutions for UAS that can add to NATO capabilities.[116] One example of potential cooperation with Israel lies in the field of inexpensive loitering munitions such as the IAI *Harpy* (which uses a passive radar

In terms of boosting reassurance and deterrence efforts in the Baltic region, NATO has a long way to go, bearing in mind the considerable Russian EW capability, since this capability feeds into Russian A2/AD approach

113. Lastochkin and Falichev, "Oruzhiye asimmetrichnogo otveta", op. cit.; Valagin, "Strategicheskaya sistema REB", op. cit.; Tikhanychev, "O roli sistematicheskogo ognevogo vozdei'stviya", op. cit.
114. Ellen Mitchell, "Army's electronic-warfare training seen as lagging behind Russian efforts", *Inside Defense*, December 8, 2015, https://insidedefense.com/inside-army/armys-electronic-warfare-training-seen-lagging-behind-russian-efforts (accessed July 10, 2017).
115. Author interviews with NATO EW specialists, Brussels, June 2017.
116. Author interviews with Israeli defence specialists, Washington DC, June 2017.

seeker), which should be prioritised by the Alliance given the limited Suppression of Enemy Air Defences (SEAD) capabilities of NATO's European members. Joint development of a home-on-jam loitering munition should be considered, as this could potentially prove a very effective and relatively low-cost solution against Russian noise jammers.[117]

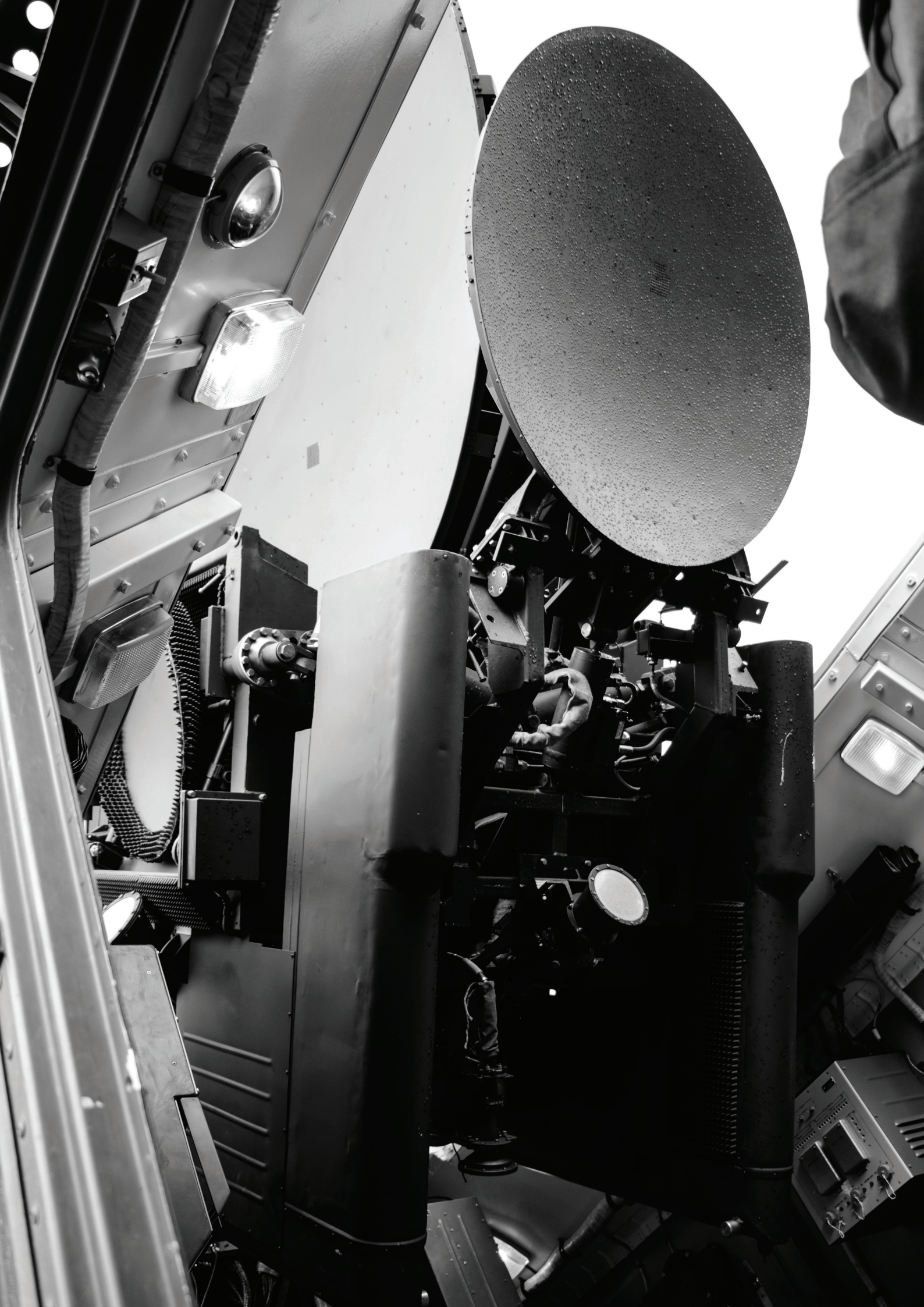
However, the Alliance will have to look initially to boost the EW capabilities of the Baltic states and enhance defence against a growing Russian A2/AD capability, as well as take into account Moscow's efforts to modernise and integrate C4ISR in its range of offensive hard-power tools. Russia's advances in EW, which add depth and credibility to its A2/AD approach, will in turn compel NATO to work on the problem framed less as a kinetic issue (bombs on target) than as a kinetic/non-kinetic integration issue (utilising space, cyber and the EMS) to find new vectors to gain access. This will also involve creating a C2 structure that allows commanders and their planners at the operational level the authority (really tactical control) to integrate diverse capabilities within a timeline that can take advantage of opportunities as they present themselves on the battlefield.[118] In the air domain, for example, NATO has enjoyed robust tactical networks to provide situational awareness and connect the tactical assets directly to operational decision-makers in real time. Operating in an EMS-challenged environment would be both unique and difficult. NATO militaries perhaps need to examine tactical connectivity in the way air superiority is considered—to create pockets of connectivity at specific times in specific locations to enable operations.[119]

The Alliance will have to look initially to boost the EW capabilities of the Baltic states and enhance defence against a growing Russian A2/AD capability

Moscow has embarked on a policy of technological catch-up, even with its limited means and the many challenges mitigating against the wider recovery of its domestic defence industry, yet the gap is narrowing in key areas and will close altogether unless NATO reacts to Russia's programme of rebuilding its conventional offensive capability. Moreover, and equally important, it has introduced a more flexible stance in its doctrinal approaches, to complement EW development. The paradigm shift in Russia's approach to warfighting to one similar to NATO's and the adoption of EW as a key enabler through networked C2 and integration of these very capable threat systems, coupled with advanced IW, could level the playing field between NATO and Russia very quickly in any future conflict. Russia's EW capability should be viewed not just in terms of EW, but as electromagnetic manoeuvre in a contested EMS battlespace. As a result, if this analysis is correct, more than any other factor in the development of Russia's conventional military capability, EW poses a fundamental and long-term challenge to the Alliance.

The paradigm shift in Russia's approach to warfighting and the adoption of EW as a key enabler could level the playing field between NATO and Russia very quickly in any future conflict

117. These munitions are designed to detect and destroy GPS jammers.
118. Author interviews with NATO EW specialists, Brussels, June 2017.
119. Author interviews with NATO EW specialists, Brussels, June 2017.



List of References

Alexeyev, Alex. "Voyna v efire. Chast' 1" [War on airwaves. Part 1]. *Voyennoye Obozreniye*, May 22, 2017. https://topwar.ru/116054-voyna-v-efire-chast-1.html. Accessed July 10, 2017.

AO "Nauchno-tekhnicheskiy tsentr radio-eletronnoy bor'by" [JSC Scientific-technical centre for electronic warfare]. Accessed July 10, 2017. http://www.ntc-reb.ru/.

Bartles Charles K., Roger N. McDermott. "Russia's Military Operation in Crimea: Road-Testing Rapid Reaction Capabilities". *Problems of Post-Communism*, Vol. 61, No. 6 (2014): 46–63.

Baulin V., A. Kondratyev. "Realizatsiya kontseptsii 'setetsentricheskaya voyna' v VMS SShA" [Implementation of "network-centric warfare" concept in the US Navy]. *Zarubezhnoye Voyennoe Obozreniye*, No. 6, June 2009. http://pentagonus.ru/publ/26-1-0-811. Accessed July 10, 2017.

Boltunov, M.. *Zolotoye ukho voyennoy razvedki* [A golden ear of military intelligence]. Moscow: Veche, 2011.

Borisov, Yuriy and Oleg Falichev. "Tyazhelaya raketa nelegkoy sud'by" [Heavy rocket of a difficult fate]. *Voyenno-Promyshlennyy Kuryer*, May 11, 2016. http://vpk-news.ru/articles/30571. Accessed July 10, 2017.

Bozhyeva, Olga. "Festival' 'novaya voyna'" [Festival "New War"]. *Moskovskiy Komsomolets,* October 17, 2009. http://www.mk.ru/editions/daily/article/2009/10/08/364473-festival-novaya-voyna.html. Accessed July 10, 2017.

Burenok, Vasiliy, Alexey Kravchenko and Sergey Smirnov. "Kurs–na setetsentrcheskuyu sistemu vooruzheniya" [The course set towards network-centric system of armaments]. *Vozdushno-Kosmicheskaya Oborona*, May 2009. http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya. Accessed July 10, 2017.

Burenok, Vasiliy. "Bazis setetsentricheskih voyn—operezhenie, intellekt, innovatsii" [The basis of network-centric wars—advance, intellect, innovations]. *Nezavisimoye Voyennoe Obozreniye,* April 2, 2010. http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html. Accessed July 10, 2017.

Chernysheva, Olga. "Obnaruzheniye i podavleniye" [Detection and suppression]. *Na Strazhe Zapolyariya*, December 4, 2015.

Denisentsev, Sergey. "Okno vozmozhnostey dlya REB" [Window of opportunity for EW]. *Voyenno-Promyshlennyy Kuryer*, 2 July 2014. http://www.vpk-news.ru/articles/20874. Accessed July 10, 2017.

Dobykin, V.D., A.I. Kupriyanov, V.G. Ponomarev and L.N. Shustov. *Radioelektronnaya bor'ba. Silovoe porazhenie radioelektronnykh sistem* [Electronic warfare. Kinetic strikes on electronic systems]. Moscow: Vuzovskaya kniga, 2007.

"'Dobyto v shakhte': Na vooruzhenii terroristov LNR stoit rossiyskaya perenosnaya stantsiya razvedki 'Kredo-M1'. Foto" ["Mined from a mine": weaponry of LNR terrorists includes a Russian mobile reconnaissance station *Kredo-M1*. A photo]. *Begemot*, March 26, 2017. http://begemot.media/news/dobyto-v-shahte-na-vooruzhenii-terroristov-lnr-stoit-rossijskaya-perenosnaya-stantsiya-razvedki-kredo-m1-foto/. Accessed July 10, 2017.

"Electronic warfare by drone and SMS: How Russia-backed separatists use 'pinpoint propaganda' in the Donbas". *Atlantic Council's Digital Forensic Research Lab*, May 18, 2017. https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696. Accessed July 10, 2017.

"Electronic warfare: How to neutralize the enemy without a single shot". *Vesti*, April, 17, 2017. http://www.vesti.ru/doc.html?id=2878732&cid=4441. Accessed July 10, 2017.

Garavskiy, Andrey. "Svyaz' reshaet vse" [Communications determine everything]. *Krasnaya Zvezda,* June 4, 2010. http://old.redstar.ru/2010/05/22_05/1_01.html. Accessed July 10, 2017.

Gavrilov, Yuriy. "Podrazdeleniya elektronnoy voyny proveli obucheniye v Severnoy Osetii" [Electronic warfare units conducted exercises in South Ossetia]. *Rossiyskaya Gazeta*, June 26, 2015.

Gordiyenko, Vladimir. "Stoletiye radioelektronnoy bor'by" [Centenary of electronic warfare]. *Nezavisimoye Voyennoye Obozreniye*, April 11, 2003. http://nvo.ng.ru/history/2003-04-11/5_reb.html. Accessed July 10, 2017.

Gusarov, Vyacheslav. "Osobennosti organizatsii i vedeniya radioelektronnoy bor'by v boyakh za Ilovaysk. Analitika IS" [Peculiarities of battle order and conduct of electronic warfare in the battles for Ilovaysk. Analysis of IS]. *Informatsionnoye Soprotivleniye,* December 5, 2016. http://sprotyv.info/ru/news/kiev/osobennosti-organizacii-i-vedeniya-radioelektronnoy-borby-v-boyah-za-ilovaysk-analitika. Accessed July 10, 2017.

—. "Taktika rossiyskikh grupp REB v boyakh za Debal'tsevo. Analitika IS" [Tactics of the Russian EW groups in the battles for Debaltsevo. Analysis of IS]. *Informatsionnoye Soprotivleniye*, January 5, 2017. http://sprotyv.info/ru/news/kiev/taktika-rossiyskih-grupp-reb-v-boyah-za-debalcevo-analitika.

Ivanov, I.A. and I. Chadov. "Soderzhanie i rol' radioelektronnoy bor'by v operatsiyakh XXI veka" [The contents and role of electronic warfare in the operations of the 21st century]. *Zarubezhnoye Voyennoye Obozreniye* No. 1 (2011): 14–20. Accessed July 10, 2017. http://pentagonus.ru/publ/soderzhanie_i_rol_radioehlektronnoj_borby_v_operacijakh_xxi_veka/80-1-0-1700.

Khudoleev, Viktor. "Voyska dlya srazheniya v efire" [Troops for combat on airwaves]. *Krasnaya* Zvezda, April 14, 2014. www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire. Accessed July 10, 2017.

Kipp, Jacob W.. "Confronting the RMA in Russia". *Military Review* 77(3) (1997): 49–55. Accessed July 10, 2017. http://fmso.leavenworth.army.mil/documents/confront.htm.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva and Jenny Oberholtzer. *Lessons from Russia's Operations in Crimea and Eastern Ukraine.* Santa Monica, CA: RAND, 2017.

Kolesova, N.A. and G. Nasenkova (eds.). *Radioelektronnaya bor'ba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego* [Electronic Warfare. From the Experiments of the Past to the Future Decisive Front]. Moscow: CAST, 2015.

"Kompleks 'Krasukha' polnost'yu oslepil istrebiteli na ucheniyakh ZVO" [Complex *Krasukha* has completely blinded fighter jets during the exercises of Western MD]. *RIA Novosti*, August 14, 2015. https://ria.ru/defense_safety/20150814/1183503352.html. Accessed July 10, 2017.

Korolyov, I., S. Kozlitin and O. Nikitin. "Problemy opredeleniya sposobov boevogo primeneniya sil i sredstv radioelektronnoy bor'by" [Problems of determining ways of employing forces and means of electronic warfare]. *Voyennaya Mysl'* No. 9 (2016): 14–19.

Kozhevnikov, Sergey. "Radioelektronnaya bor'ba v gody Velikoy Otechestvennoy voyny" [Electronic warfare during the years of Great Patriotic war]. *Belorusskaya Voyennaya Gazeta*, April 16, 2014. https://vsr.mil.by/2014/04/16/radioelektronnaya-borba-v-gody-velikoj-otechestvennoj-vojny/. Accessed July 10, 2017.

"Krasukha-4 v Sirii: god elektronnogo shchita na Khmeymim" [*Krasukha-4* in Syria: a year of electronic shield over Khmeimim]. *Defence.ru*, October 11, 2016. https://defence.ru/article/krasukha-4-v-sirii-god-elektronnogo-schita-nad-khmeimim/. Accessed July 10, 2017.

"KRET v 2015 godu peredal Vooruzhennym Silam 9 kompleksov REB Moskva-1" [In 2015, KRET handed over to the Armed Forces 9 complexes of EW *Moskva*-1]. *RIA Novosti*, December 25, 2015. http://ria.ru/defense_safety/20151225/1348750286.html. Accessed July 10, 2017.

KRET. "REB dlya chaynikov" [EW for dummies]. Last modified January 18, 2016, accessed July 10, 2017. http://kret.com/media/news/reb-dlya-chaynikov/.

—. "The upgraded *Rychag*-AV system will be produced in 2016-17". Last modified September 27, 2015, accessed July 10, 2017. http://oblik.msk.ru/en/news/4002/.

Kruglov, E.. 'Perspektivy razvitiya amerikanskikh sredtsv REB i taktika ikh primeneniya v sovremennykh vooruzhonnykh konfliktakh' [Prospects of development of the American EW means and tactics of their employment in contemporary armed conflicts]. *Zarubezhnoye Voyennoye Obozreniye* No. 2 (2014): 57–63. Accessed July 10, 2017. http://pentagonus.ru/publ/perspektivy_razvitija_amerikanskikh_aviacionnykh_sredstv_rehb_i_taktika_ikh_primenenija_v_sovremennykh_vooruzhjonnykh_konfliktakh_2014/18-1-0-2480.

Kudryavtsev, Aleksandr. "Tenevyye storony radioelektronnoy bor'by" [Shadowy sides of electronic warfare]. *Voyennoye Obozrenye*, December 22, 2013. http://topwar.ru/37601-tenevye-storony-radioelektronnoy-borby.html. Accessed July 10, 2017.

Lastochkin, Yuriy. "Ni dnya bez pomekh" [Not a day without interferences]. *Voyenno-Promyshlennyy Kuryer,* April 27, 2016. http://www.vpk-news.ru/articles/30428. Accessed July 10, 2017.

—. "Rol' i mesto radioelektronnoy bor'by v sovremennykh i budushchikh boyevykh deystviyakh" [Role and place of electronic warfare in contemporary and future combat actions]. *Voyenayya Mysl'* No. 12 (2015): 14–19.

Lastochkin, Yuriy and Oleg Falichev. "Kupol nad Minoborony" [A dome above the Ministry of Defence]. *Voyenno-Promyshlennyy Kuryer,* April 26, 2017. http://www.vpk-news.ru/articles/36422. Accessed July 10, 2017.

—. "Oruzhiye asimmetrichnogo otveta" [Weapons of asymmetric response]. *Voyenno-Promyshlennyy Kuryer,* May 14, 2014. http://vpk-news.ru/articles/20241. Accessed July 10, 2017.

Litovkin, Nikolay. "Russia receives first Il-22PP *Porubschik* electronic countermeasures planes". *Russia Beyond the Headlines*, November 9, 2016. https://www.rbth.com/defence/2016/11/09/russia-receives-first-il-22pp-porubschik-electronic-countermeasures-planes_646271. Accessed July 10, 2017.

Livejournal. "19-ya otdel'naya brigada radioelektronnoy bor'by" [19th separate electronic warfare brigade]. Accessed May 19, 2017. http://bmpd.livejournal.com/1852552.html.

MacFarquhar, Neil. "U.S. agrees with Russia on rules in Syrian sky". *New York Times,* October 20, 2015. www.nytimes.com/2015/10/21/world/middleeast/us-and-russia-agree-to-regulate-all-flights-over-syria.html?_r=0. Accessed July 10, 2017.

Majumdar, Dave. "The Russian Military's 5 Next Generation Super Weapons". *The National Interest*, November 8, 2015. http://nationalinterest.org/blog/the-buzz/the-russian-militarys-5-next-generation-super-weapons-14276. Accessed July 10, 2017.

McDermott, Roger N.. *Brothers Disunited: Russia's Use of Military Power in Ukraine*. Fort Leavenworth: Foreign Military Studies Office, 2015. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/197162. Accessed July 10, 2017.

Mikhaylov, Andrey. "Pyatidnevnaya voyna: itog v vozdukhe" [Five-day war: outcome in the air]. *Vozdushno-Kosmicheskaya Oborona*, January 30, 2009. http://www.vko.ru/voyny-i-konflikty/pyatidnevnaya-voyna-itog-v-vozduhe. Accessed July 10, 2017.

Ministerstvo Oborony Rossiyskoy Federatsii. "Voyennyy Entsiklopedicheskiy Slovar'" [Military Encyclopedic Dictionary]. Accessed May 19, 2017. http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14416@morfDictionary.

Ministerstvo Oborony Rossiyskoy Federatsii. "V obshchevoyskovoy armii ZVO provedena trenirovka grupp po bor'be s bespilotnikami" [In the combined-arms army of Western MD, training exercises were conducted for counter-UAV groups]. Last modified June 29, 2017, accessed July 10, 2017. http://function.mil.ru/news_page/country/more.htm?id=12131418@egNews.

Mitchell, Ellen. "Army's electronic-warfare training seen as lagging behind Russian efforts". *Inside Defense*, December 8, 2015. https://insidedefense.com/inside-army/armys-electronic-warfare-training-seen-lagging-behind-russian-efforts. Accessed July 10, 2017.

"Moscow, Minsk to jointly prepare electronic warfare structure". *Interfax*, June 8, 2011. http://www.interfax.com/newsinf.asp?id=250211. Accessed July 10, 2017.

"Na vooruzheniye ZVO postupil kompleks REB Borisoglebsk-2" [EW complex *Borisoglebsk*-2 entered service in Western MD]. *Zvezda,* April 1, 2017. https://tvzvezda.ru/news/opk/content/201704011213-cqzx.htm. Accessed July 10, 2017.

Nagalin, A., Y. Donskov and I. Anisimov. "Iyerarkhiya tseley i zadach, vozlagayemykh na podrazdeleniya REB v obshchevoyskovom boyu" [The hierarchy of objectives and tasks given to EW units in combined-arms warfare]. *Voyennaya Mysl'*, No. 4 (2013): 77–84.

"Navy responds to claim ship was scared off by Russian jets with video". *Foxtrotalpha*, June 1, 2015, http://foxtrotalpha.jalopnik.com/navy-responds-to-claim-ship-was-scared-off-by-russian-j-1708178476. Accessed July 10, 2017.

Novichkov, Nikolai. "Russia receives new Mi-8MTPR-1 electronic warfare helicopters". *Jane's Defence Weekly*, March 4, 2015.

Opall-Rome, Barbara. "Russia, Israel to broaden coordination in Syria". *OSnet Daily*, December 1, 2015. http://osnetdaily.com/2015/12/russia-israel-to-broaden-coordination-in-syria/. Accessed July 10, 2017.

OSCE Special Monitoring Mission to Ukraine. "Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 14 May 2017". Last modified May 15, 2017, accessed July 10, 2017. http://www.osce.org/special-monitoring-mission-to-ukraine/317386.

Paliy A.I.. "Radioelektronnaya bor'ba v khode voyny" [Electronic warfare in the course of war]. *Voyenno-Istoricheskiy Zhurnal* No. 5 (1976): 10–16.

—. *Ocherki istorii radioelektronnoi bor'by* [Essays on the history of electronic warfare]. Moscow: Vuzovskaya kniga, 2006.

—. *Radioelektronnaya bor'ba v voynakh i vooruzhennykh konfliktakh* [Electronic warfare in wars and armed conflicts]. Moscow: VAGSH, 2007.

"Radioelektronnaya bor'ba rossiyskikh terroristicheskikh sil v nachal'noy faze voyennogo konflikta v Ukraine" [Electronic warfare by the Russian terrorist forces during the initial phase of the armed conflict in Ukraine]. *Informatsionnoye Soprotivleniye*, September 20, 2016. http://sprotyv.info/ru/news/kiev/radioelektronnaya-borba-rossiyskih-terroristicheskih-sil-v-nachalnoy-faze-voennogo. Accessed July 10, 2017.

Radziyevskiy, V.G.. *Sovremennaya radioelektronnaya bor'ba. Voprosy metodologii* [Contemporary electronic warfare. Issues of methodology]. Moscow: Radiotekhnika, 2006.

Ramm, Aleksey. "Elektronnaya voyna—mify i pravda (Part 1)" [Electronic warfare—myths and the truth]. *Voyenno-Promyshlennyy Kuryer*, September 30, 2015. http://vpk-news.ru/articles/27272. Accessed July 10, 2017.

—. "Elektronnaya voyna—mify i pravda (Part 2)" [Electronic warfare—myths and the truth]. *Voyenno-Promyshlennyy Kuryer*, October 6, 2015. http://vpk-news.ru/articles/27410. Accessed July 10, 2017.

—. "Razrabotchik sistem REB: Amerikanskiye Tomagavki—slozhnyye tseli" [Developer of EW systems: American Tomahawks—difficult targets]. *Izvestiya*, April 14, 2017. http://izvestia.ru/news/683822. Accessed July 10, 2017.

Ramm, Aleksey, Dmitriy Litovkin and Yevgeniy Andreyev. "V voyska radioelektronnoy bor'by pridet iskusstvennyy intellect" [Electronic warfare troops will be joined by artificial intelligence]. *Izvestiya*, April 4, 2017. http://izvestia.ru/news/675891. Accessed July 10, 2017.

Ramm, Alexey and Yevgeny Andreyev. "'Letayushchikh Medvedey usilyat 'Porubshchikami'" ["Flying Bears" will be reinforced by *Porubshchik*]. *Izvestiya*, March 31, 2016. https://iz.ru/news/674705. Accessed July 10, 2017.

"Razvedyvatel'nyye samolety, sistemy radioelektronnoy bor'by i vysokotekhnologichnaya voyna Rossii v Sirii" [Reconnaissance aircraft, electronic warfare systems and Russia's high-tech war in Syria]. *Russia Insider*, October 31, 2015. http://russia-insider.com/ru/oborona-i-bezopasnost/razvedyvatelnye-samolety-sistemy-radioelektronnoy-borby-i. Accessed July 10, 2017.

Robinson, Paul. "Explaining the Ukrainian Army's Defeat in Donbass in 2014". In J.L. Black and Michael Johns (eds). *The Return of the Cold War: Ukraine, the West and Russia*. London: Routledge, 2016.

"Rossiya mozhet ispol'zovat' v Sirii samolet A-50" [Russia might use aircraft A-50 in Syria]. *Rossiyskaya Gazeta*, January 14, 2016. https://rg.ru/2016/01/14/a50-site-anons.html. Accessed July 10, 2017.

"Russia's fake 'electronic bomb': How a fake based on a parody spread to the Western mainstream". *Atlantic Council's Digital Forensic Research Lab*, May 9, 2017. https://medium.com/dfrlab/russias-fake-electronic-bomb-4ce9dbbc57f8. Accessed July 10, 2017.

"Russian Armed Forces: *Moskva*-1 Systems Can 'Target' Up To Nine Electronic Warfare Systems". *RIA Novosti*, December 25, 2015.

"Russian jamming system blocks all NATO electronics over Syria". *Sputnik*, October 29, 2015. http://in.sputniknews.com/world/20151029/1016211289/russian-jamming-system-syria-nato.html. Accessed July 10, 2017.

Ryabchuk, V.D., et al., *Elementy voyennoy sistemologii primenitel'no k reshenyu problem operativnogo iskusstva i taktiki obshchevoyskovykh ob'edineniy, soyedineniy i chastey: Voyenno-teoreticheskiy trud* [Elements of military system applicable to solving problems of operational art and tactics of combined-arms formations and units: Military-theoretical work]. Moscow: Izdatel'stvo Akademii, 1995.

Ryabchuk, V.D.. "Nauka, obrazovaniye, reforma" [Science, education, reform]. *Voyennaya mysl'* No. 2 (1994): 39–41.

Saltykov, Yevgeniy. "Bitva za efir: rossiyskiye sistemy REB pokazali v Sirii svoyu effektivnost'" [Battle for airwaves: Russian EW systems showed their effectiveness in Syria]. *Vesti*, March 18, 2016, http://www.vesti.ru/doc.html?id=2732816. Accessed July 10, 2017.

Sharkovskiy, Aleksandr. "Skromnyy potentsial kompleksa Zaslon-REB" [Modest potential of the complex *Zaslon*-REB]. *Nezavisimoye Voyennoye Obozreniye*, April 20, 2017. http://www.ng.ru/armies/2017-04-20/2_6978_zaslon.html. Accessed July 10, 2017.

Shepovalenko, M.Y. (ed.). *Siriyskiy Rubezh* [Syrian Frontier]. Moscow: CAST, 2016.

Shepovalenko, Maksim. "Boevye lazery budushchikh voyn" [Combat lasers of future wars]. *Voyenno-Promyshlennyy Kuryer*, July 3, 2013. http://www.vpk-news.ru/articles/16579. Accessed July 10, 2017.

Silyuntsev, V., V. Demin and D. Prokhorov. "Boyevoye primeneniye REB" [Combat application of EW]. *Armeyskiy Sbornik* No. 7 (2016): 43-53. Accessed July 10, 2017. http://sc.mil.ru/files/morf/military/archive/AC_07_2016.pdf.

Simonov, Andrey, Denis Khripushin and Mikhail Chikin, "Perspektivy avtomatizirovannogo upravleniya v soyedineniyakh radioelektronnoy bor'by Vooruzhonnykh Sil Rossiyskoy Federatsii" [Prospects of automated command and control in the formations of electronic warfare of the Armed Forces of the Russian Federation]. *Materialy ot voysk radioelektronnoy bor'by VS RF* No. 1 (2017): 38-39. Accessed May 12, 2017. https://reb.informost.ru/2017/pdf/1-7.pdf.

"Sovremennym rossiyskim sredstvam REB pod silu 'vyrubit'' tselyy polk" [Modern Russian EW means are capable of "switching off" an entire regiment]. *Voyennoye Obozreniye*, December 10, 2014. https://topwar.ru/64421-sovremennym-rossiyskim-sredstvam-reb-pod-silu-vyrubit-celyy-polk.html. Accessed July 10, 2017.

"Spetsialnye ucheniya Elektron-2016 provodyatsya na yuge Rossii" [Special exercises *Elektron*-2016 are conducted in the south of Russia]. *Zashchishchat' Rossiyu*, August 19, 2016. https://defendingrussia.ru/a/cpecialnyje_uchenija_elektron2016_prohodjat_na_juge_rossii-6207/. Accessed July 10, 2017.

Tikhanychev, O.V.. "O roli sistematicheskogo ognevogo vozdei'stviya v sovremennykh operatsiyakh" [On the role of a systematic fire support impact in contemporary operations]. *Voennaya Mysl'*, No. 11 (2016): 16-20.

Tikhonov, Aleksandr. "V tsentre vnimaniya oboronka" [Defence industry in focus]. *Krasnaya Zvezda*, May 12, 2016. http://redstar.ru/index.php/component/k2/item/28841-v-tsentre-vnimaniya-oboronka. Accessed July 10, 2017.

Tsvetnov, V.V., V.P. Demin and A.I. Kupriyanov. *Radioelektronnaya bor'ba. Radiomaskirovka i pomekhozashchita* [Electronic warfare. Electronic camouflage and defence against interference]. Moscow: MAI, 1999.

—. *Radioelektronnaya bor'ba. Radiorazvedka i radioprotivodeystviye* [Electronic warfare. Electronic intelligence and electronic counter-measures]. Moscow: MAI, 1998.

"Turetskiy Korall protiv rossiyskogo Triumfa: sistemy REB u granits Sirii" [Turkish *Korall* against the Russian *Triumf*: EW systems on the borders of Syria]. *Voyennoye Obozreniye,* December 3, 2015. http://topwar.ru/87224-tureckiy-korall-protiv-rossiyskogo-triumfa-sistemy-reb-u-granic-sirii.html. Accessed July 10, 2017.

"Ucheniya voysk REB Zapadnogo voyennogo okruga" [Exercises of EW troops in Western Military District]. *Voyennoye Obozreniye,* July 22, 2016. https://topwar.ru/98370-ucheniya-voysk-reb-zapadnogo-voennogo-okruga.html. Accessed July 10, 2017.

"V Sirii poyavilos' rossiyskoye radioelektronnoye oruzhiye—Times" [Russia's electronic weapons appeared in Syria—Times]. *KorrespondenT.net*, October 7, 2015. http://korrespondent.net/world/3573109-v-syryy-poiavylos-rossyiskoe-radyoelektronnoe-oruzhye-Times. Accessed July 10, 2017.

"V Siriyu pribyli noveyshyye rossiyskiye kompleksy radioelektronnoy bor'by 'Krasukha-4'" [The newest Russian electronic warfare complexes *Krasukha-4* arrived at Syria]. *Voyennyy Informator*, October 5, 2015. http://military-informant.com/airforca/v-siriyu-pribyili-noveyshie-rossiyskie-kompleksyi-radioelektronnoy-borbyi-krasuha-4.html. Accessed July 10, 2017.

"V Vooruzhennykh Silakh Rossiyskoy Federatsii otmechayetsya Den' Spetsialista po Radioelektronnoy Bor'be" [Russian Federation Armed Forces mark the Day of Electronic Warfare Specialist]. *Eurasian Defence,* April 15, 2017. http://eurasian-defence.ru/?q=node/38809. Accessed July 10, 2017.

"V Zapadnyy voyennyy okrug prishla novaya tekhnika radioelektronnoy bor'by" [New electronic warfare equipment arrives at Western Military District]. *Voyennoe.rf,* December 19, 2016. http://www. военное.рф/2016/3во62/. Accessed July 10, 2017.

Valagin, Anton. "Chto napugalo amerikanskii esminets" [What scared the American destroyer]. *Rossiyskaya Gazeta*, April 30, 2014. www.rg.ru/2014/04/30/reb-site.html. Accessed July 10, 2017.

—. "Strategicheskaya sistema REB podavit svyaz' NATO" [Strategic system of EW will suppress NATO's communications]. *Rossiyskaya Gazeta*, November 14, 2016. https://rg.ru/2016/11/14/strategicheskaia-sistema-reb-podavit-sviaz-nato.html. Accessed July 10, 2017.

Vladykin, Oleg. "Plashchi-nevidimki dlya tankov, korabley i samoletov" [Invisibility cloaks for tanks, ships and aircraft]. *Nezavisimoye Voyennoye Obozreniye*, January 29, 2017. http://www.ng.ru/week/2017-01-29/8_6915_army.html. Accessed July 10, 2017.

Voyskovye Chasti Rossii. "15-ya otdel'naya brigada radioelektronnoy bor'by" [15th separate electronic warfare brigade]. Accessed July 10, 2017. http://voinskayachast.net/suhoputnie-voyska/specialnie/vch71615.

ANNEX A

Spectrum of EM Emissions and Use for Military and Civilian Purposes[120]

Frequency Band		Waveband		Use	
Band Name	Frequency	Waveband	Wave name	Civilian	Military
Radio Band					
	Up to 300 mHz	Up to 1 Mm	Infrasonic		Seismic and acoustic weaponry
HLF (ГНЧ)	300-3000 mHz	1-10 Mm	Hectomegametric		
ELF (КНЧ)	3-30 Hz	10-100Mm	Decamegametric	Geophysical research	
SLF (СНЧ)	30-300 Hz	1000-10,000 km	Megametric		Communications with submarines
ULF (ИНЧ)	300-3000 Hz	100-1000 km	Hectokilometric		
VLF (ОНЧ)	3-30 KHz	10-100 km	Miriametric (superlong)	Hydroacoustic stations	
LF (НЧ)	3-300 KHz	1-10 km	Kilometric (long)	Radionavigation systems	
MF (СЧ)	300-3000 KHz	100-1000 m	Hectometric (medium)	Radio broadcasting, maritime mobile communications	
HF (ВЧ)	3-30 MHz	10-100 m	Decametric (short)	Radio broadcasting, maritime mobile comms, medical ultrasonic scanners	Tactical level radio comms, over-the-horizon radar
VHF (ОВЧ)	30-300 MHz	1-10 m	Metric (ultrashort)	Radio, television broadcasting	Tactical level radio comms, long-range radar detection
UHF (УВЧ)	300-3000 MHz	1-10 dm	Decimetric	Satellite navigation systems, satellite communication systems	
				Network communications, maritime mobile comms, television broadcasting	Missile attack early warning system, mobile radio frequency
SHF (СВЧ)	3-30 GHz	1-10 cm	Centimetric	Satellite communication systems, radio relay communications, tropospheric communications, wireless computer networks	
				Civilian radar (support for navigation and air control)	Military radar (detection of ground, surface and aerial targets, fire control
EHF (КВЧ)	30-300 GHz	1-10 mm	Millimetric	Radio-astronomical, high-speed radio relay communications, civil radar (meteorology)	Mobile radio frequency weapon systems, military radar (tracking ballistic missile and space objects, reconnaissance of moving ground targets), automated data transmission systems, broadband communications systems
HHF (ГВЧ)	300-3000 GHz	0,1-1 mm	Decimillimetric	Examination scanners, medical tomography	High-speed communication and location systems for high-altitude and space

120. Shepovalenko, “Boevye lazery budushchikh voyn”.

Frequency Band		Waveband		Use	
Band Name	Frequency	Waveband	Wave name	Civilian	Military
Radio Band					
	Up to 300 mHz	Up to 1 Mm	Infrasonic		Seismic and acoustic weaponry
HLF (ГНЧ)	300-3000 mHz	1-10 Mm	Hectomegametric		
ELF (КНЧ)	3-30 Hz	10-100Mm	Decamegametric	Geophysical research	
SLF (СНЧ)	30-300 Hz	1000-10,000 km	Megametric		Communications with submarines
ULF (ИНЧ)	300-3000 Hz	100-1000 km	Hectokilometric		
VLF (ОНЧ)	3-30 KHz	10-100 km	Miriametric (superlong)	Hydroacoustic stations	
LF (НЧ)	3-300 KHz	1-10 km	Kilometric (long)	Radionavigation systems	
MF (СЧ)	300-3000 KHz	100-1000 m	Hectometric (medium)	Radio broadcasting, maritime mobile communications	
HF (ВЧ)	3-30 MHz	10-100 m	Decametric (short)	Radio broadcasting, maritime mobile comms, medical ultrasonic scanners	Tactical level radio comms, over-the-horizon radar
VHF (ОВЧ)	30-300 MHz	1-10 m	Metric (ultrashort)	Radio, television broadcasting	Tactical level radio comms, long-range radar detection
UHF (УВЧ)	300-3000 MHz	1-10 dm	Decimetric	Satellite navigation systems, satellite communication systems	
				Network communications, maritime mobile comms, television broadcasting	Missile attack early warning system, mobile radio frequency
SHF (СВЧ)	3-30 GHz	1-10 cm	Centimetric	Satellite communication systems, radio relay communications, tropospheric communications, wireless computer networks	
				Civilian radar (support for navigation and air control)	Military radar (detection of ground, surface and aerial targets, fire control

ANNEX B

RUSSIAN EW SYSTEMS

EW System	Purpose
RB-301B	Designed to jam HF/VHF/UHF communications. Includes: RK-330KMV command post; R-378BMV, R-330BMV, R-934BMV and R-325UMV jamming stations. http://www.sozvezdie.su/newspaper/_22_dekabr_2009_g/borisoglebsk2__noviy_kompleks/ http://www.efirzavod.ru/index.php?id=37
1L269 Krasukha-2-O	Designed to jam S-band radars (typically employed by AEW&C aircraft). http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-krasukha-2-o/
1RL257 Krasukha-C4	Designed to jam X/Ku-band fire control radars (typically employed by fighter aircraft). http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-krasukha-s4/
Moskva-1	ESM system. Includes: 1L265 passive detection station. Detection, identification of direction-finding of airborne radar emissions. 1L266 command post for controlling jamming stations designed to jam airborne radars. http://kret.com/products/radioelektronnaya-borba/stantsiya-radioelektronnoy-razvedki-moskva-1e/
SPR-2M Rtut-BM	Designed to jam communications, radio-proximity fuses and remote detonator signals. http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-rtut-bm/
RB-531B Infauna	Designed to jam communications, radio-proximity fuses and remote detonator signals. Also features optical detection of missile launches and automatic release of smoke. https://rg.ru/2014/04/30/reb-site.html
Lesochek	Designed to jam communications, radio-proximity fuses and remote detonator signals. Compact - man portable. https://rg.ru/2014/04/30/reb-site.html
Pole-21	Designed to jam GPS signals. Includes R-340RP jamming stations that are mounted on cell mobile phone towers. http://iz.ru/news/628766#ixzz4IHrzF0Xl
RP-377LA Lorandit	Designed for detection, direction-finding and jamming of HF/VHF/UHF communications. https://reb.informost.ru/2014/pdf/1-8.pdf http://forums.airbase.ru/2014/05/t89725--sredstva-reb-i-rtr-podrazdelenij-vdv.html
Magniy-REB	Designed for training EW specialists. http://syria.mil.ru/news/more.htm?id=12054820@egNews
Leer-2	Designed to jam communications. http://www.armyrecognition.com/russia_russian_army_wheeled_armoured_vehicle_uk/tigr-m_mktk_rei_pp_leer-2_vpk-233114_mobile_electronic_warfare_ew_vehicle_technical_data_sheet.html
RB-341V Leer-3	Designed to jam GSM networks. Includes a command post and three Orlan-10 UAVs equipped with jammers. Also capable of transmitting SMS messages to mobile phones. Leer-3s have apparently been upgraded to work with 3G and 4G networks as well; however this has not been verified. http://iz.ru/news/659503
Less	Automated command post. Designed to collect and process data, and control electronic protection/ electromagnetic emission control systems. https://reb.informost.ru/2014/pdf/1-8.pdf
RB-636M2 Svet-KU	Electronic protection/electromagnetic emission system. Designed for evaluation of electromagnetic situation. Conducts detection, analysis and direction-finding of emitting sources. https://reb.informost.ru/2014/pdf/1-8.pdf http://bastion-karpenko.ru/svet-ku/
Alurgit	No reliable information about this system could be found.
Parodist	No reliable information about this system could be found.

Follow us on:

facebook.com/ICDS.Tallinn
Twitter: @ICDS _ Tallinn
linkedin.com/company/3257237

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

ISSN 2228-0529
ISBN 978-9949-9885-9-4 (print)
978-9949-9972-0-6 (PDF)